2013-1489

IN THE

UNITED STATES COURT OF APPEALS

FOR THE FEDERAL CIRCUIT

VIRNETX, INC.,

and

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION,

Plaintiffs-Appellees,

v.

CISCO SYSTEMS, INC.,

Defendant,

and

APPLE INC.,

Defendant-Appellant.

Appeal from the United States District Court for the Eastern District of Texas in case no. 10-CV-0417, Chief Judge Leonard Davis.

CORRECTED NON-CONFIDENTIAL BRIEF FOR PLAINTIFFS-APPELLEES VIRNETX INC. AND SCIENCE APPLICATIONS INTERNATIONAL CORPORATION

J. Michael Jakes
Kara F. Stoll
Srikala Atluri
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP
901 New York Avenue, NW
Washington, DC 20001
(202) 408-4000

Benjamin R. Schlesinger
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP
3500 SunTrust Plaza
303 Peachtree Street, NE
Atlanta, GA 30308-3263
(404) 653-6400

[Counsel Continued]

Bradley W. Caldwell
Jason D. Cassady
John Austin Curry
CALDWELL, CASSADY & CURRY
2101 Cedar Springs Rd.
Suite 1000
Dallas, TX 75201
(214) 888-4848

Attorneys for VirnetX Inc.

Donald Urrabazo
Arturo Padilla
Ronald Wielkopolski
URRABAZO LAW, P.C.
2029 Century Park East
Suite 1400
Los Angeles, CA 90067
(310) 363-9088

Andy Tindel
MANN, TINDEL & THOMPSON
112 E Line Street, Suite 304
Tyler, TX 75702
(903) 596-0900

Attorneys for Leidos, Inc., formerly Science Applications International Corporation

December 2, 2013

CERTIFICATE OF INTEREST

Pursuant to Federal Circuit Rule 47.4, counsel of record for Plaintiff-Appellee VirnetX Inc. certify as follows:

1. The full name of every party or amicus represented by us is: VirnetX Inc.

2. The name of the real party in interest represented by us is: VirnetX Inc.

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by us are: VirnetX Inc. is a wholly owned subsidiary of VirnetX Holding Corporation ("VHC"). VHC's stock is publicly traded on the New York Stock Exchange.

4. The names of all law firms and the partners or associates that appeared for the parties represented by us in the trial court, or are expected to appear in this Court, are:

   Finnegan, Henderson, Farabow, Garrett & Dunner, LLP: J. Michael Jakes, Kara F. Stoll, Srikala P. Atluri, and Benjamin R. Schlesinger

   Caldwell, Cassady, & Curry: Bradley W. Caldwell, Jason D. Cassady, and John Austin Curry

CERTIFICATE OF INTEREST

Pursuant to Federal Circuit Rule 47.4, counsel of record for Plaintiff-Appellee Leidos, Inc., formerly Science Applications International Corporation, certify as follows:

1. The full name of every party or amicus represented by us is: Leidos, Inc. is the represented party. Science Applications International Corporation ("SAIC") was recently renamed Leidos, Inc. as part of a corporate reorganization. This name change did not effect Leidos, Inc.'s interest in the patents at issue.

2. The name of the real party in interest represented by us is: Leidos, Inc. is the real party in interest. Science Applications International Corporation ("SAIC") was recently renamed Leidos, Inc. as part of a corporate reorganization. This name change did not effect Leidos, Inc.'s interest in the patents at issue.

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by us are: Leidos Holdings, Inc. owns 100% of Leidos, Inc. SAIC, Inc. and Science Applications International Corporation were recently renamed Leidos Holdings, Inc. and Leidos, Inc., respectively, as part of a corporate reorganization. This name change did not effect Leidos, Inc.'s interest in the patents at issue.

4. The names of all law firms and the partners or associates that appeared for the parties represented by us in the trial court, or are expected to appear in this Court, are:

   URRABAZO LAW, P.C.: Donald Urrabazo, Arturo Padilla, Ronald Wielkopolski

   MANN, TINDEL & THOMPSON: Andy Tindel

TABLE OF CONTENTS

CONFIDENTIAL MATERIAL OMITTED

The material omitted on page 16 describes a sealed Apple document. The material omitted on page 70 describes the results of internal Apple customer surveys. This material was designated confidential by Appellant Apple Inc. pursuant to the Protective Order entered August 2, 2011, and amended March 5, 2012.

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

FEDERAL RULES

OTHER AUTHORITIES

STATEMENT OF RELATED CASES

No other appeal from the same Civil Action No. 10-CV-417 (E.D. Tex.) was previously before this Court or any other appellate court. The following cases known to counsel involve one or more of the patents-in-suit (U.S. Patent Nos. 6,502,135 ("the '135 patent"); 7,490,151 ("the '151 patent"); 7,418,504 ("the '504 patent"); and 7,921,211 ("the '211 patent")) or patents related to the patents-in-suit, and may be directly affected by the Court's decision in this appeal:

VirnetX, Inc. v. Apple Inc., No. 13-cv-211 (E.D. Tex.)

VirnetX, Inc. v. Apple Inc., No. 12-cv-855 (E.D. Tex.)

VirnetX, Inc. v. Apple Inc., No. 11-cv-563 (E.D. Tex.)

VirnetX, Inc. v. Cisco Sys., Inc., No. 10-cv-417 (E.D. Tex.)

VirnetX, Inc. v. Microsoft Corp., No. 13-cv-351 (E.D. Tex.)

I. STATEMENT OF JURISDICTION

VirnetX agrees with Apple's Statement of Jurisdiction except for Apple's assertion that the district court's judgment is non-final. It is final for the reasons the district court noted in its opinion (A83-88), consistent with *Robert Bosch, LLC v. Pylon Manufacturing Corp.*, 719 F.3d 1305 (Fed. Cir. 2013).

II. COUNTERSTATEMENT OF THE ISSUES

1. Did the district court correctly deny JMOL of noninfringement of the '135 and '151 patents where substantial evidence supports that VPN On Demand (1) performs the "determining whether" element; and (2) initiates a VPN, secure channel, and encrypted channel "between" the client and target computer or secure server?
2. Did the district court correctly deny JMOL of noninfringement of the '504 and '211 patents where the court properly construed the terms "domain name" and "secure communication link," and substantial evidence supports that FaceTime uses "direct communication," as Apple advocated in the construction of "secure communication link"?
3. Did the district court correctly deny JMOL of invalidity where substantial evidence supports that Kiuchi does not teach (1) "direct communication" between a client and target; and/or (2) "storing a plurality of domain names and corresponding IP addresses"?

4. Did the district court properly exclude non-final reexamination evidence that was more prejudicial than probative?

5. Did the district court err in denying Apple's damages JMOL and motion for new trial when properly admitted theories support the award?

III. COUNTERSTATEMENT OF THE CASE

A. Preliminary Statement

Seeking to overturn the jury verdict, Apple raises numerous issues and only tells half the story for each. With little room in its brief to educate the Court on all issues, Apple does not even begin to identify evidence the jury reasonably relied on to find infringement, no anticipation, and damages. Nor does Apple address intrinsic evidence supporting the district court's claim construction. Further, although nearly all contested issues are reviewed for substantial evidence or abuse of discretion, Apple treats them like legal issues, ignoring this Court's standard of review. As discussed below, substantial evidence supports the jury verdict on infringement, anticipation, and damages, and Chief Judge Davis properly exercised his discretion on evidentiary issues. Moreover, the intrinsic and extrinsic evidence supports the court's construction of "domain name" and "secure communication link," limitations from two of the four patents-in-suit.

B. Course of Proceedings and Disposition Below

This appeal is from a final judgment in a patent case. After the court construed the claims, the case proceeded to trial. The parties presented expert

testimony and other evidence to the jury over five days. The jury found infringement of all asserted patents, none of the claims invalid, and awarded damages of $368,160,000. A240-41.

IV. COUNTERSTATEMENT OF THE FACTS

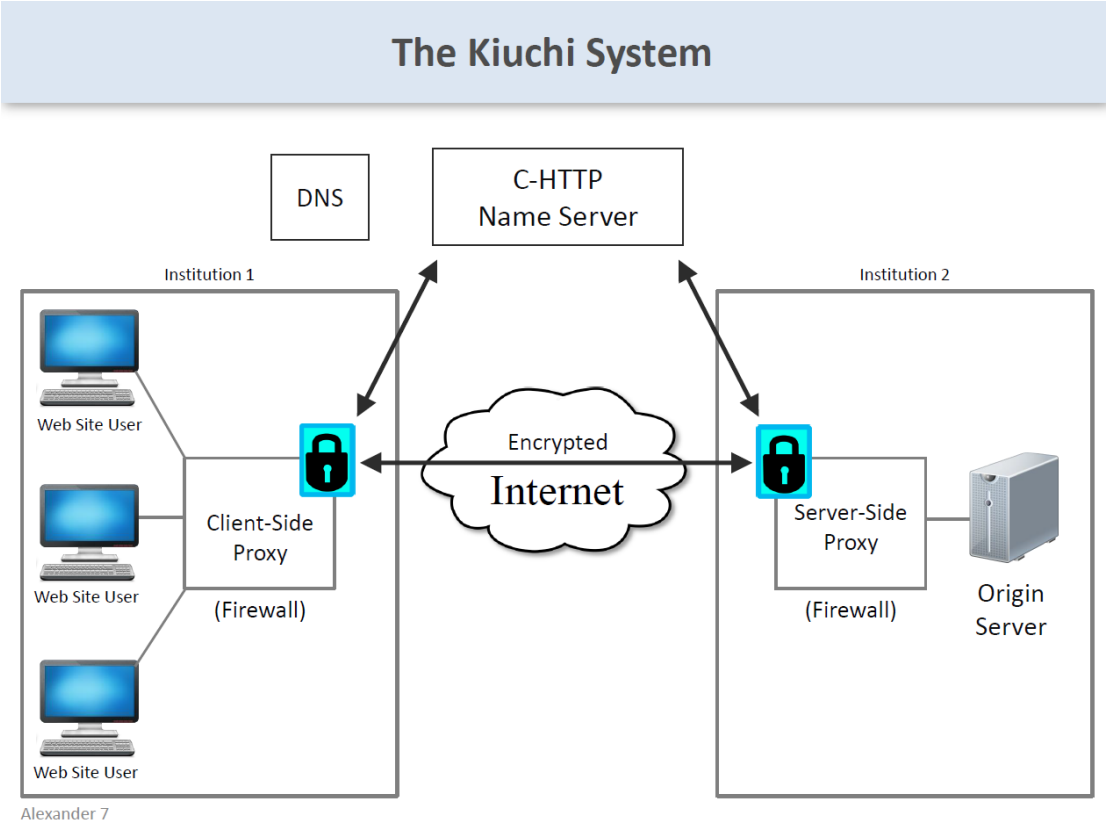
A. Background

1. The Problem: Secure Communications on Unsecured Networks

During Gulf War I, the military faced a critical problem: using unsecured commercial satellites to communicate sensitive data. A1072:9-1074:4. The military turned to Science Applications International Corporation ("SAIC"), a company providing technology solutions to organizations like the CIA. SAIC tasked Dr. Bob Short and Mr. Gif Munger with building a secure satellite network using unsecured satellites. A1072:3-1074:4; A1186:16-1187:25.

At the time, many different solutions attempted to provide security over public networks like the Internet. For example, Kiuchi—the prior art Apple relies on—taught a technique called "closed HTTP" ("C-HTTP") for communications between hospitals. In Kiuchi, C-HTTP allowed website users at one hospital to retrieve information from another hospital's network. A15008. As depicted below, the website user could not *directly* access resources in the other hospital's network. Instead, communications between the website user and origin server were proxied by the client-side and server-side proxy servers, which terminated the

connection, wrapped/unwrapped the messages, encrypted/decrypted the contents, reformatted, and re-sent the messages. A15009-10. Furthermore, as Kiuchi recognizes, this solution was not commercially viable. A15012-13("Our system is assumed to accommodate up to a few hundred[] proxies[,] much smaller than that needed for most commercial purposes.").



Apple Trial Demonstrative

Other solutions involved virtual private networks ("VPNs"). As its name suggests, a *virtual* private network extends a private network across the Internet or other public network. It enables a computer outside a private network to send and

receive data across public networks as if it were directly connected to the secure private network. A1323:23-1324:2.

After successfully completing the satellite project, Short and Munger continued providing communication security to CIA operatives, inventing a complex type of VPN (called a TARP VPN in the patents-in-suit). A1075:4-1076:3; A1081:7-24. In-Q-Tel, a company Congress established to identify and develop emerging technologies, granted a $3.5M contract to SAIC to continue developing that VPN in exchange for a 3% royalty. A1084:5-1085:9; A1596:14-20.

In developing the TARP VPN, Short and Munger recognized that setting up even a normal VPN was complex—requiring configuration of security, encryption, and network parameters on either side of the connection. A1081:22-1083:11; A1193:9-1195:16; A20241. They appreciated that users would use secure connections like VPNs only if they were easy or automatic. A1083:5-19; A1195:11-21.

2. The Inventors Solve the Problem

While returning from an In-Q-Tel contract kick-off meeting, Short had his "aha" moment. Recognizing that users were accustomed to entering domain names to initiate Internet communications, Short conceived of using a domain name to trigger secure communications. A1087:9-1089:8; A1195:22-1198:7. The

other inventors immediately knew this was the elegant solution they sought. A1197:18-1198:18. Over the next several months, they fleshed out implementation details, and eventually applied for and received multiple patents. A1094:22-1098:3; A1197:18-1199:23; A242-529. Within SAIC, the project was called "VirnetX," meaning "virtual network exchange." A1013:25-1014:3.

B. VirnetX's '135 and '151 Patents

1. Common Specification

The '135 and '151 patents disclose a novel system in which a Domain Name Server ("DNS") proxy automatically and transparently creates a VPN in response to a DNS lookup. A298(37:17-21). As background, conventional DNSs are used in the Internet to resolve domain names (e.g., "Yahoo.com")[1] into Internet Protocol ("IP") addresses. *Id.*(37:22-27). A web browser then uses the IP address to request a website. *Id.*(37:24-29).

Figure 26 depicts an embodiment in the patents. A273; A298(38:14-15).

[1] The patents list "Yahoo.com" as an example domain name in a "conventional scheme," but recognize domain names may be any name corresponding to an IP address. A298(37:33-36); A303(47:24-25, 39); A446(37:4-6).

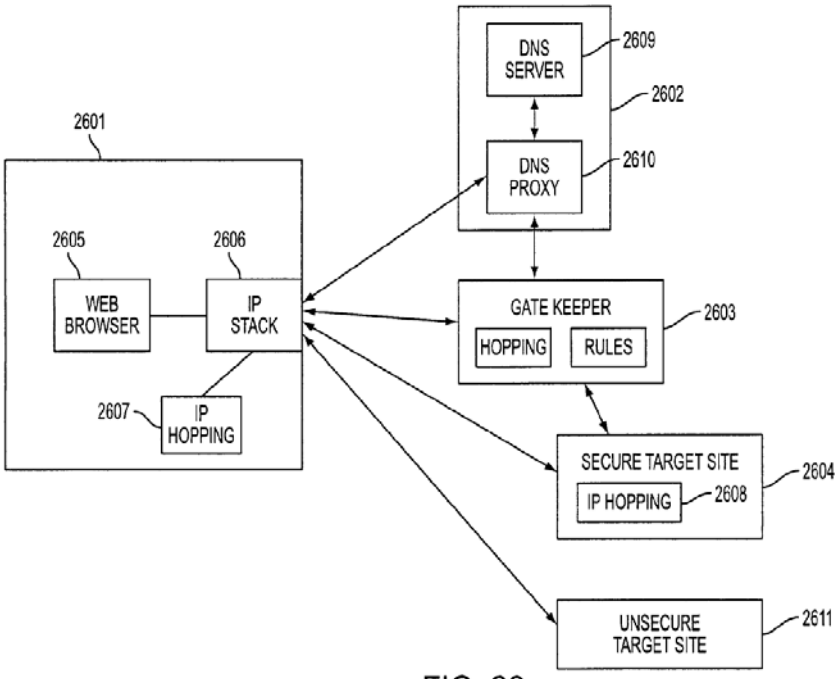


FIG. 26

Browser (2605) within user computer (2601) generates a domain name service request when a domain name is entered. Instead of conventional DNS (2609) receiving the request, DNS proxy (2610) intercepts it and determines whether the request is for a secure site. A298(38:23-25). According to a preferred embodiment, this determination is made by checking the domain name against a table of domain names. *Id.*(38:23-30(whether "access to a secure site has been requested" is determined "by reference to an internal table of such sites")).

If the domain name is listed, DNS proxy (2610) determines the request is requesting access to a secure site and automatically initiates a VPN between browser (2605) and secure target site (2604). *Id.*(38:25-33). If the domain name is not listed, DNS proxy (2610) determines that the request is not seeking access to a

secure site and forwards the request to conventional DNS (2609) for resolution (without initiating a VPN). *Id.*(38:43-47).

2. Asserted Claims

At trial, VirnetX asserted that Apple's VPN On Demand products infringed '135 patent claims 1, 3, 7, and 8, and '151 patent claims 1 and 13. '135 patent claim 1 is representative:

> A method of transparently creating a virtual private network (VPN) between a client computer and a target computer, comprising the steps of:
>
> (1) generating from the client computer a Domain Name Service (DNS) request that requests an IP address corresponding to a domain name associated with the target computer;
>
> (2) *determining whether the DNS request transmitted in step (1) is requesting access to a secure web site*; and
>
> (3) in response to determining that the DNS request in step (2) is requesting access to a secure target web site, *automatically initiating the VPN between the client computer and the target computer*.

A303(47:20-32). Italics represent limitations Apple contends are not met.

'151 patent claims 1 and 13 are similar to '135 patent claim 1, except they require "initiating an encrypted path" and "secure channel," respectively, instead of a "VPN." A450(46:55-67); A451(48:18-29).

C. VirnetX's '504 and '211 Patents

1. Common Specification

The '504 and '211 patents share the same specification and disclose a novel domain name service system that, unlike conventional DNS, resolves domain names beyond just simple web pages on the Internet and facilitates establishing secure communication links. A383(49:1-6). The "secure communication link" of the '504 and '211 patents is not the same as the "VPN" communication of the '135 patent. The '504 and '211 patents explain that, "[a]ccording to one variation of the invention," a secure communication link *can be* augmented to become a VPN, making clear a VPN is just one *type* of secure communication link. *Id.*(49:37-45); A383-84(50:58-51:7, 51:62-52:2). Notably, the specification does not equate the broad language "secure communication link" to a VPN, but instead discloses that there are "[a] tremendous variety of methods" to provide secure communication. A359(1:33-35).

The specification explains the domain name service system may be used, "for example," in "the situation when computer network 3302 is the Internet" (A383(49:26-30)), thus contemplating networks other than the Internet. Indeed, it contemplates using the invention for secure communication between "application programs [that] include video conferencing, e-mail, word processing programs, telephony, and the like." A369(21:27-29); *see id.*(21:12-15).

Figure 33 depicts one preferred embodiment of this novel system (A383(49:12-15); A354):

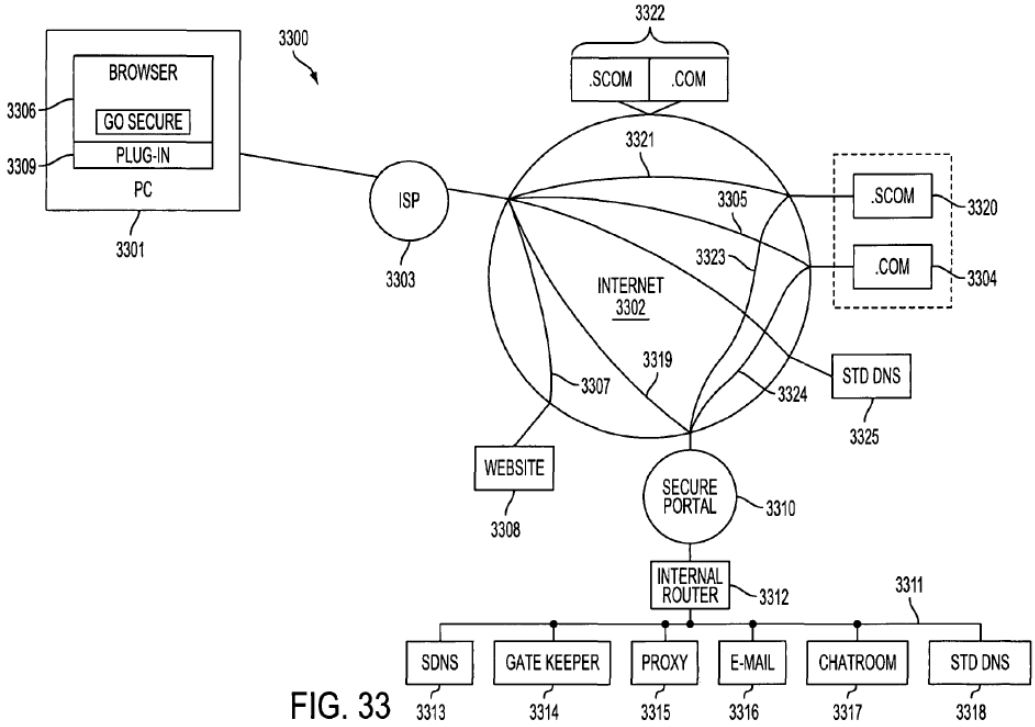


FIG. 33

To establish a secure communication link between client computer (3301) and target computer (3304), an application on client computer (3301) sends a query including a domain name. A383(50:54-57); A384(51:29-32). In this embodiment, Secure Domain Name Service (3313), which "contains a cross-reference database of secure domain names and corresponding secure network addresses," receives the query. A384(51:11-15). A secure communication link is then established between client computer (3301) and target computer (3304) associated with the network address. *Id.*(51:34-40).

2. Asserted Claims

At trial, VirnetX asserted that Apple's FaceTime products infringe '504 patent claims 1, 2, 5, 16, 21, and 27, and '211 patent claims 36, 37, 47, and 51. '504 patent claim 1 is representative:

> A system for providing a domain name service for establishing a *secure communication link*, the system comprising:
>
> a domain name service system configured
>
> to be connected to a communication network,
>
> to store a plurality of *domain names* and corresponding network addresses,
>
> to receive a query for a network address, and
>
> to comprise an indication that the domain name service system supports establishing a *secure communication link*.

A386(55:49-56). Apple contests the construction of italicized limitations.

Because Apple relies on a related patent—U.S. Patent No. 8,051,181—and its prosecution history to construe a term (B.Br.40-41), a brief discussion is helpful. The Examiner had rejected claims in the '181 patent in view of Aventail, which discloses a "SOCKS" protocol for communicating between a client on a public network and a target on a private network. A7157. The protocol requires an intermediate SOCKS proxy server between the client and target. *Id.*

During prosecution, VirnetX explained that while Aventail's SOCKS protocol allows for communication between public and private networks, it does

not allow *direct* communication such that the client and target are able to "communicate with each other as though they were on the same network." A7155. Instead, all communications "start and stop at the intermediate SOCKS server," resulting in multiple connections or communications between the client device, SOCKS server, and target device. A7157. Continuing, VirnetX explained that, given the indirect configuration required by the SOCKS protocol, "one skilled in the art would not have considered the client and target to be virtually on the same private network. Instead, the client computer and target computer are deliberately separated by the intermediate SOCKS server." *Id*.

Based on this, and at Apple's urging, the court below construed a "secure communication link" to be direct. A11-13. The court understood that VirnetX's statements did not equate a "secure communication link" with a "virtual private network communication link" (A11-12), as Apple now argues.

VirnetX also discussed the disputed term "domain name" during the '181 patent's prosecution. Specifically, VirnetX explained a "secure name" can be a "secure domain name," which can include "*a telephone number*." A20836(emphasis added). In a subsequent reexamination requested by

Apple, Apple and the Examiner repeatedly relied on this representation. A20879; A20881; A20888; A20890; A20846.[2]

D. VirnetX Is Formed to Implement the Inventions

After filing their patent applications, the inventors searched for ways to implement their technology in a product. Because SAIC was not in the business of bringing products to market, they looked for outside help. A1103:19-1104:13. Before issuance of the patents, they received their first chance at implementation with SafeNet, a network security company. SafeNet agreed to integrate VirnetX's technology into its software and pay SAIC a 20% royalty. A1105:4-1106:6; A20245-76. Unfortunately, SafeNet abandoned the project due to the dotcom bust of the early 2000s combined with the complexity of implementation. A1106:8-1107:5("Our technology took the complexity away from the user, but it didn't make the complexity go away. It went into the software.").

During this time, Munger introduced VirnetX's technology to businessman Kendall Larsen. A1210:21-1213:8. Impressed, Larsen left his job to raise the necessary capital without pay, ultimately incorporating VirnetX in 2005. A1213:9-1214:19; A1216:22-1228:12. As its first order of business, VirnetX licensed and

[2] This Court may take judicial notice of statements made during prosecution and reexamination of the '181 patent. *See, e.g., St. Clair Intellectual Prop. Consultants, Inc. v. Canon Inc.*, 412 F. App'x 270, 275 n.1 (Fed. Cir. 2011)(taking judicial notice of reexamination record).

later purchased the asserted patents from SAIC, agreeing to a 15% royalty on any commercialization with a maximum payment amount for certain activities. A1228:13-1229:20; A20277-314; A20329-42.

1. VirnetX Begins to Implement the Inventions

Once VirnetX acquired patent rights, it identified Microsoft Windows as the initial platform to launch its security product. A1231:1-10. SAIC and VirnetX continued on the project, but halfway through, they learned Microsoft had already incorporated VirnetX's technology in its products. A1231:11-1232:14. Realizing it would be difficult to compete with Microsoft, SAIC reached out to Microsoft in 2006, but the infringing use was not resolved for several years. A1110:20-1111:5; A1114:4-1115:9; A1232:15-22.

Notwithstanding Microsoft's then-unlicensed use, VirnetX was determined to develop a product, which it named "Gabriel." Gabriel's development continued and, in 2010, VirnetX and Microsoft reached an agreement. A1114:10-1115:9; A1115:3-13; A20343-55. For $200M, VirnetX granted Microsoft a limited field-of-use license. Specifically, VirnetX retained for itself an exclusive market to provide, *inter alia*, secure domain name services that establish secure communication links between Microsoft and non-Microsoft products or between non-Microsoft products. A1233:18-1234:13; A20345; *see also* A1115:10-1116:8.

Immediately after signing the agreement, VirnetX refocused Gabriel and began optimizing it for the mobile market. A1234:24-1235:14. In particular, VirnetX sought to secure communications on the popular Apple iPhone. A1235:15-21. VirnetX discovered, however, that Apple was already using its inventions. A1235:22-1236:1. Thus, despite VirnetX's efforts to carve out an exclusive market for Gabriel, it found itself, yet again, up against an industry giant who already had a foothold in the market using VirnetX's technology. A1236:2-9. VirnetX filed this suit to regain the exclusivity conferred by its patent rights and create a marketplace for Gabriel. *See* A1127:2-5. While spending a significant portion of time focusing on protecting its intellectual property, VirnetX continued developing Gabriel on several platforms, which it demonstrated to the jury. *See* A1119:25-1121:21.

2. VirnetX's Licensing Policy and Other Licenses

Prior to the Microsoft agreement, VirnetX developed a licensing policy. A1238:3-14. The policy provides for standard (2-5%) and incentivized (1-2%) running royalty rates applied to the total value of the licensed product, and was influenced by the previous personal patent-licensing experience of VirnetX's CEO. A1208:9-1209:25; A1238:9-1241:22. In 2010, VirnetX signed its limited license with Microsoft for a lump sum of $200M, which equates to less than 1%. A1245:3-10; A20343-55. VirnetX gave Microsoft this "special deal" because it

was VirnetX's first deal (providing further validation for the technology), the scope of the license was limited, and VirnetX was nearly out of money at the time. A1233:4-1234:23; A1245:11-1246:14; A1298:12-1299:3. Every other license, however, strictly complied with VirnetX's licensing policy, including agreements with Aastra, Mitel, and NEC in 2012. *See, e.g.*, A1242:23-1243:17; A20356-80; A20388-411; A20424-53. These companies agreed to royalty rates between 1-1.61% based on their total product revenue for licensed secure voice-over-Internet phones and servers, including devices offering video-conferencing. A1243:13-17; A1601:4-16; A2310:11-17; A20357-58; A20365-66; A20389-90; A20396-97; A20425-26; A20432-37.

E. Apple's Accused Products

1. VPN On Demand Products

VirnetX accused Apple's products that implement VPN On Demand—including select iPhone, iPad, and iPod Touch products ("iOS devices")—of infringing the '135 and '151 patents. A1375:23-1376:11. VPN On Demand cannot be purchased separately for any iOS device. A1376:12-16.

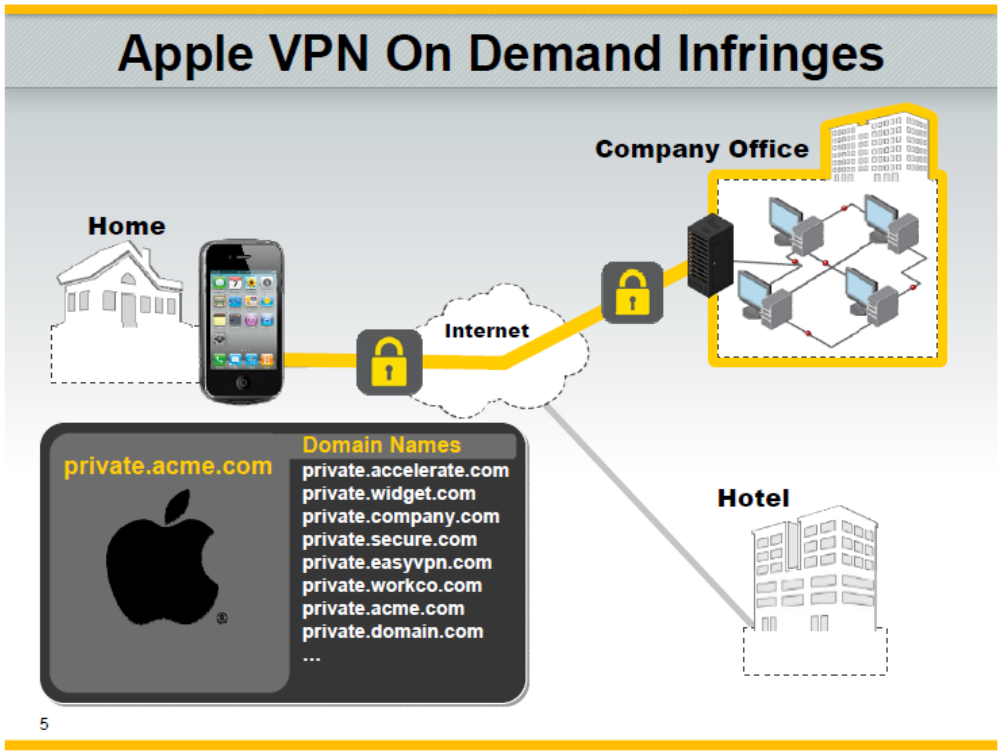
Apple [redacted] "[c]oncerns over security" [redacted]. A20230; A1383:13-1385:17. With VPN On Demand, "[s]ecure access to private corporate networks is available" using "established

industry-standard VPN protocols." A20001. Apple touts "[u]sers can easily connect to enterprise systems via the built-in VPN client." *Id.*

Apple's VPN On Demand feature is accessed every time a domain name is entered into the Safari browser of an iOS device. A1377:8-1378:12. Once a domain name is entered, a domain name service request is generated. A1393:22-1394:8. Like the preferred embodiment of the '135 and '151 patents, VPN On Demand receives the request and checks a list of domain names in a configuration file to "determine if [the entered domain name] is a domain or a subdomain that is behind a private network." A1406:7-19(Apple witness Howard Ridenour); A1377:8-1378:1; A15238. The list contains domain names for which a VPN should be established. A1377:8-22. While nothing prohibits a user from misconfiguring this list by entering public domain names, Apple's planning documents, internal emails, and presentations uniformly explain VPN On Demand is intended to "[c]onnect VPN automatically when an application tries to access a resource in a *private network*"—i.e., a secure website. A15236(emphasis added); A15055; A15490; A1402:25-1405:22(VirnetX's expert Jones); A1406:7-19(Ridenour).

If the entered domain name matches one on the list, VPN On Demand contacts a VPN server to authenticate the user. A1396:19-1398:11. A VPN is then automatically established between Safari and the resource in the secure private

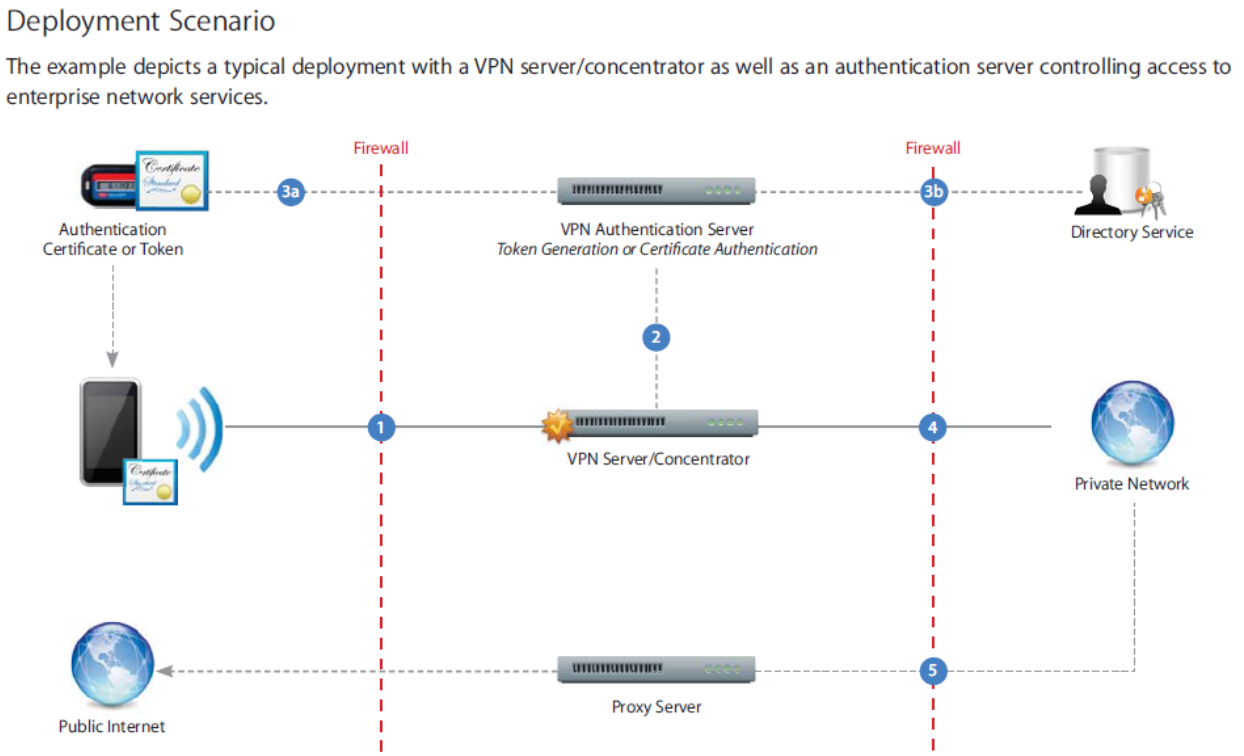
network. A15236; A1398:16-1401:23. This VPN uses encryption to provide anonymity and security for the insecure path between Safari and the VPN server, as depicted below in yellow. A1378:23-1379:8; A1400:18-1401:11.



VirnetX Trial Demonstrative

Behind the VPN server, the VPN relies on the private network to provide anonymity and security. A1379:9-14; A1401:12-18; A20003. According to Apple's product specifications and marketing presentations, VPN On Demand is designed to connect with *secure* private or "corporate" networks that require authentication for access. *See* A20001(for private corporate networks "where certificate-based authentication is used, iPhone features VPN On Demand"); A15055; A15057(corporate environments use secure Wi-Fi deployment);

A1379:15-17. As shown in the Figure below, these documents further disclose that, in a "typical deployment scenario" for VPN On Demand, the private network includes multiple layers of security, including VPN servers, VPN authentication servers, firewalls, and proxy servers. A20003; A15056; A2001:9-2002:17(Apple's expert Kelly).



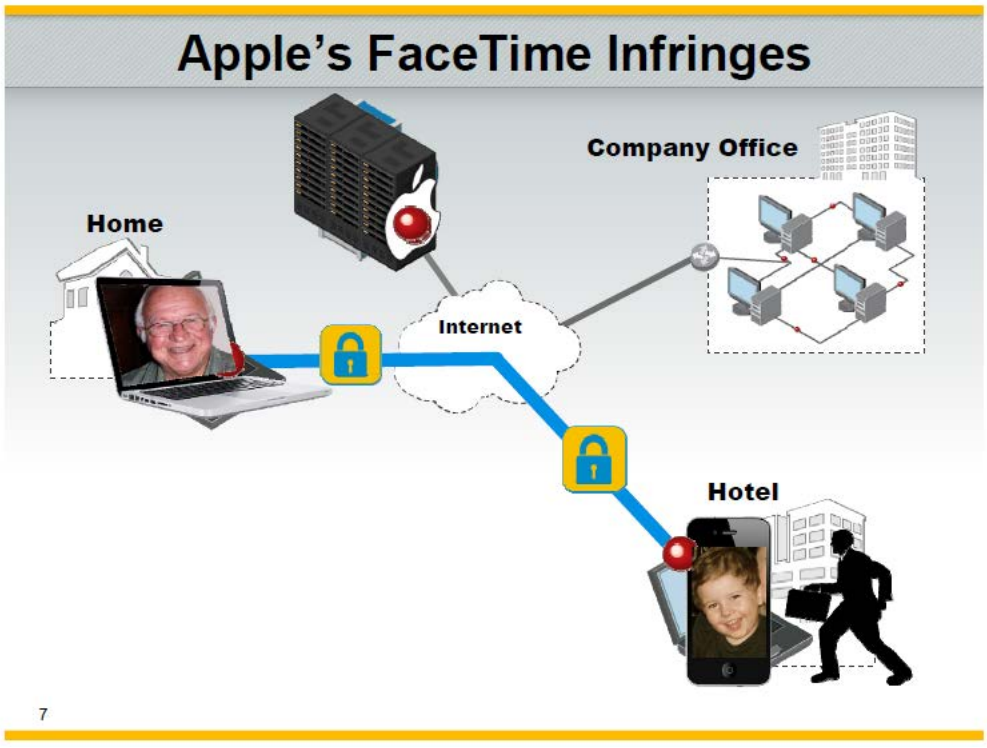
VPN On Demand Deployment Scenario

2. FaceTime Products

VirnetX accused Apple's products that implement FaceTime—including select Mac computers and iOS devices—of infringing the '504 and '211 patents. A1315:19-1316:15. While FaceTime cannot be separately added to any iOS

device, FaceTime was made available as an operating system ("OS") upgrade to Mac computers. A1619:15-22; A1719:18-1720:9.

FaceTime allows secure video calling between select Apple devices. A1443:11-18. To use FaceTime, a caller enters a recipient's email address or phone number into his device (e.g., his Mac). A1451:21-1452:20. The recipient can accept or decline the call at his device (e.g., his iPhone). A1452:25-1453:14. If accepted, Apple's FaceTime servers provision the devices to establish an encrypted FaceTime call. A1453:15-1454:12; A20055. Audio/video data are sent in packets across the encrypted communication path, depicted below in blue. A1450:9-25; A1465:17-20.



VirnetX Trial Demonstrative

According to Apple's technical and marketing presentations, FaceTime "[c]reates *direct* peer-to-peer connections" that are "encrypted end to end." A15449(emphasis added); A15167; A15394; A15479; A15485; A20055; A20711; A20724. Apple's documents explain, however, that communication "[f]alls back to a relay server if direct connectivity fails." A15394; A15449; A20718. At the time of trial, 5-10% of FaceTime calls were made using a relay server. A1446:10-19. Relayed calls involve not only readdressing the packets, but also terminating FaceTime communication at the relay and maintaining separate communications with each Apple device, thus resulting in an indirect connection. A1445:15-1446:1; A1565:2-12; A1573:23-1574:9. It is undisputed that FaceTime calls via relay server are indirect and not accused of infringement. A1916:20-25(Kelly).

The remaining 90-95% of FaceTime calls, however, were direct via network address translation ("NAT") routers. A1446:10-24. NAT routers interface between wide area networks ("WANs") like the Internet and local area networks ("LANs") like those found in users' homes. A1536:10-1537:7; A1785:22-1787:7(Gates). A NAT router receives FaceTime data packets having a transport address that allows the router to identify a particular device (e.g., an iPhone) in a LAN. A1467:16-25(Jones); A1969:21-1970:2(Kelly). The NAT router then translates the transport address from the WAN, a public address space, to the LAN, a private address space. A1536:10-25. Unlike Kiuchi and Aventail proxy servers

and FaceTime relay servers, NAT routers do not terminate the connection, and the communication remains direct between caller and recipient. A1443:24-1446:24; A1461:15-1469:17; *see also* A1982:3-1984:19(Kelly); A1778:15-1787:7(Gates).

F. District Court Proceedings

1. Infringement Evidence: ’135 and ’151 Patents

a. “Determining Whether”

VirnetX’s expert, Dr. Jones, explained to the jury that VPN On Demand checks a configuration list to determine whether the domain name service request is for a secure website. A1377:8-1378:12; A1394:18-1398:15; A1880:19-1881:2(Kelly); A2005:4-11(Ridenour). He explained that, “of course,” Apple knows that VPN On Demand is designed to connect to existing private networks because “[t]hat’s the purpose of a VPN.” A1379:15-17.

Jones disagreed with Apple’s assertion that, “because VPN On Demand can be configured to trigger a VPN based on a website like ebay.com, that VPN On Demand just simply can’t infringe.” A1402:5-1407:9. He explained that Apple’s technical design documents show the configuration list is intended to contain “private address[es] [that] should trigger a VPN connection.” A15255; A1402:5-1407:9. He also explained that Apple’s internal technical presentations, marketing presentations, and emails indicate that VPN On Demand “[d]etermine[s] if the host is in the *private network*” (A15238(emphasis added)) and that VPN On Demand “[c]onnect[s] VPN automatically when an application tries to access a resource in a

private network" (A15236(emphasis added)). *See also* A15055; A15490(establish VPN only "to send traffic to the *corporate network*")(emphasis added); A15250("Typing a 'public' name or address in a web browser (e.g., www.apple.com) should not trigger a VPN connection, while typing a 'private' (e.g., web.apple.com) address should cause VPN [to] attempt a connection."); A20017; A20002-03.

b. Initiating VPN "Between" Client and Target

Jones testified that, with VPN On Demand, "the virtual private network extend[s] from the client computer to the target computer." A1400:18-1401:18. As he explained to the jury, the VPN extends all the way from the client to the target "because it's encrypted on the insecure paths, and it's secure within the corporate network." *Id.*

c. "Encrypted Channel Between" Client and Secure Server

Referring to '151 patent claim 1, which requires an "encrypted channel between the client and the secure server," Jones explained VPN On Demand encrypts the channel between the client and VPN server. A1423:20-1424:3. He admitted communication within the private network to the secure server is not necessarily encrypted (although it is secure) and thus relied on the doctrine of equivalents to show infringement. A1421:7-18; A1424:15-1425:7; *see also* A1400:18-1401:18. Because encryption is just one way of achieving data security,

Jones testified that encryption and physically securing a communication path are interchangeable ways of providing data security. A1421:19-24; A1424:15-25; A13("[E]ncryption is not the only means of addressing data security."). Jones also explained VPN On Demand products perform substantially the same function as the encrypted channel, namely securing communication against potential eavesdroppers, in substantially the same way, by encrypting communication on insecure paths, and achieve substantially the same result, protecting the entire path from client to secure server from potential eavesdroppers. A1424:4-25.

2. Infringement Evidence: '504 and '211 Patents

a. Construction of "Domain Name"

During the *Markman* hearing, Apple contended (as it does here) that "domain name" means "a hierarchical sequence of words in decreasing order of specificity that corresponds to a numerical IP address." A6298-300. In particular, Apple cited the specification's examples of domain names, including "Yahoo.com," and a dictionary defining domain name as "[a]n address of a network connection that identifies the owner of that address in a hierarchical format." A6299(emphasis omitted).

The court rejected Apple's attempts to limit the claims. Adopting its reasoning in *VirnetX v. Microsoft* (A5475-509), a related case involving overlapping patents, the court found the specification's reference to exemplary

domain names like "Yahoo.com" unpersuasive. A16. The court concluded that Apple, like Microsoft before it, argued "only the presence and absence of examples rather than any enforceable language of limitation." A5488; A16. The court also emphasized that "[t]he claims themselves describe 'domain name,'"; indeed, '135 patent claim 1 recites "an IP address corresponding to a domain name." A5486-87. The court found that the extrinsic dictionary definitions and expert testimony "do[] not carry great weight in light of the fact that claim language provides guidance on the meaning of 'domain name.'" A5488. Thus, it construed "domain name" as "a name corresponding to an IP address." A5489; A16.

b. Construction of "Secure Communication Link"

The parties also disputed the meaning of "secure communication link." Apple initially asserted that it required communications to be secure *and anonymous*, even though the claim says nothing about anonymity. A6297-98. For support, Apple cited statements in the specification indicating the secure communication link can be a VPN[3] and the '181 patent prosecution history (discussed *supra* 11-13). *Id*.

The court again rejected Apple's attempt to read limitations into the claims. The court noted that, while the specification indicates the "secure communication

[3] The district court construed VPN to require anonymity; thus, Apple sought to read in VPN.

link is a virtual private network communication link" (A361(6:61-62)), the statement concerned a preferred embodiment; it was not intended to limit the meaning of the broad term "secure communication link" in the context of all embodiments (A12-13).

Turning to the '181 patent prosecution history, the court found that "secure communication link," like VPN, requires direct communication between its nodes. A12. Although it recognized that VirnetX distinguished the Aventail prior art from a "secure communication link" for reasons nearly identical to those used to distinguish a VPN, the court did not construe the terms as synonyms. A11-12. Indeed, VirnetX's arguments in both instances focused on whether the communication was direct. Accordingly, the court construed "secure communication link" as "a direct communication link that provides data security." A13.

Subsequently, Apple moved for another construction of "secure communication link" as requiring "a direct communication link that provides data security *through encryption*." A7638. VirnetX did not oppose. A10001. Accordingly, the court adopted Apple's proposed construction. A7992. Despite this, Apple seeks a different construction on appeal.

c. Evidence Relating to "Domain Name" and Direct Communication

VirnetX presented evidence that Apple's FaceTime products literally infringe '504 patent claims 1, 2, 5, 16, 21, and 27, and '211 patent claims 36, 37, 47, and 51. With reference to the element "to store a plurality of domain names and corresponding network addresses," Jones explained that FaceTime servers store email addresses and phone numbers, which are domain names, and their corresponding IP addresses. A1460:9-1461:6; A20826-27.

Additionally, Jones addressed FaceTime's establishment of a "secure communication link." FaceTime communication, Jones explained, may occur via relay servers or NAT routers. He testified that, while relay servers stop and start communication, impeding direct communication, NAT routers simply route FaceTime calls and therefore provide direct communication. A1462:1-1468:8; A1573:23-1574:16; A1779:21-1787:7(Gates). He relied, *inter alia*, on Apple's internal technical presentations, technical specifications, and emails, which explain that NAT routers "[c]reate[] direct peer-to-peer connections," but "if direct connectivity fails," FaceTime will "[f]all[] back to a relay server." A15394; A15449; A15479; A15485; A20055; A20724; A20711; A20718.

3. Validity Evidence

At trial, Apple argued Kiuchi anticipated the asserted claims. In response, VirnetX presented evidence that Kiuchi did not teach "direct communication"

between the client and target. As VirnetX's expert, Jones, explained, the client in Kiuchi is the computer with an Internet browser. A2341:1-22; A2186:7-24(Alexander); *see also* A2339:7-18(Jones). Jones explained that, in Kiuchi, communication between the client and origin server is not "direct" because the client-side and server-side proxies terminate communication, process the information, and create a new connection. A2334:25-2335:22; A15009-10. Apple's expert agreed the proxies process the information and declined to opine whether communication between the client in Kiuchi and the origin server is direct. A2200:18-2201:8. Moreover, at the *Markman* hearing, when referring to Aventail, Apple admitted that servers "where all of the communications stopped at that server and then that server processed them and sent it on to another target" do not allow direct communication. A2661:6-12; A2710:4-6.

Apple attempted to show that Kiuchi teaches storing "a plurality of domain names and corresponding network addresses," as required in the asserted '504 and '211 patent claims. Relying on Kiuchi's appendix, Dr. Alexander (Apple's invalidity expert) claimed the C-HTTP name server receives a server-side proxy name and responds with the corresponding server-side proxy IP address. A2073:15-2074:8. But Jones revealed that Kiuchi's appendix is incorrect in this regard and that such a system would be unworkable. A2336:20-2338:20; *see also* A15016-17. As Jones explained, what Kiuchi actually teaches is that the C-HTTP

name server stores the name of the origin servers—not the server-side proxies—and the IP address of the server-side proxies. A2336:20-2338:20; A15009.

4. Evidence on Damages

VirnetX presented three damages theories supported by fact witnesses, expert testimony, and documentary evidence. VirnetX's main theory, as presented by its damages expert, Roy Weinstein, relied on a *Georgia-Pacific* analysis to calculate the reasonable royalty the parties would have agreed to in June 2009. A1593:6-1625:21. Weinstein concluded—and VirnetX's CEO, Larsen, confirmed—that a conservative reasonable running royalty rate is 1%. A1246:15-25; A1613:13-1614:7. He applied that rate to a royalty base comprised of only the smallest salable units of the accused products, resulting in a royalty of approximately $708M. A1621:9-1625:4; A1644:23-1645:1. As noted above, the jury awarded approximately $368M.

Weinstein testified that he based the royalty rate, in part, on six license agreements to the patents-in-suit or closely-related technology and VirnetX's licensing policy. A1595:6-1596:9; *see also supra* 5-6, 13-16. For each license, Weinstein explained in detail how it compared to the hypothetical negotiation, and Apple cross-examined him. *E.g.*, A1596:3-1601:22; A1717:6-1719:17. Larsen also testified, without objection, regarding the licenses and licensing policy, and their relation to the hypothetical negotiation on direct and cross-examination. *E.g.*,

A1228:13-1229:20; A1233:4-1234:15; A1238:3-1247:12; A1271:1-1272:4; A1299:23-1300:11. Larsen also testified that VirnetX's technology has been valued at $2-3 billion using a 1% royalty rate. A1261:23-1262:19.

Weinstein calculated the royalty base from the smallest salable units of the accused devices "to be as conservative as" possible. A1620:5-22. For iOS devices, he used the lowest price each device was ever sold, excluding every additional feature possible—which, with Apple's pricing structure, removed revenue from extra memory and accessories. *See* A1616:2-1619:12; A1620:11-22. For Mac computers, he used the software upgrade price ($29) that included FaceTime functionality. A1619:15-21; A1669:18-21. Weinstein also explained this software upgrade was not the smallest salable unit for iOS devices. Unlike Macs, accused iOS devices without FaceTime (e.g., iPhone 3GS) cannot be upgraded to add FaceTime because new hardware is required for FaceTime to operate—namely, a front-facing camera. A1719:18-1720:9.

Weinstein also presented alternative damage theories for FaceTime. His first alternative theory relies on the Nash Bargaining Solution, an economic theory by Nobel Prize winner, Dr. John Nash. A1628:14-1629:8; A20783-86. Weinstein explained that, under this theory, negotiating parties will split extra profits directly tied to the patented technology. A1630:4-1633:10. Because the profits would not exist without an agreement to integrate the technology, they are split between the

parties. The amount each party receives depends on its bargaining power, whether there are commercially viable alternatives, and whether the patentee sells a similar product. A1630:4-1632:19. Here, Weinstein explained Apple would have obtained an extra 10% because of its bargaining power at the time. A1708:5-1709:4. Based on Apple documents and testimony from an Apple employee, Weinstein calculated FaceTime's incremental value for each product. A1634:2-1636:24. After accounting for Apple's costs and the profit split, he calculated FaceTime damages to be approximately $588M. A1637:3-1638:5.

Weinstein's second alternative theory applies the entire market value rule for the portion of sales made because of FaceTime to calculate a per-unit-royalty. To determine that portion of sales, Weinstein considered several Apple consumer surveys, ultimately using an iPod Touch survey. A1638:20-1641:5; A1642:12-1643:5. Using the number of iPod Touches sold due to FaceTime, the associated profits, and a Nash Bargaining Solution split for those profits, Weinstein calculated a per-unit-royalty. A1641:16-1642:11. He explained that the iPod Touch survey provided the most conservative approach, despite some surveys reporting smaller numbers because other products were more expensive and had higher profit margins. A1642:17-1643:5. Applying the per-unit-royalty to the number of accused products sold containing FaceTime resulted in FaceTime damages of approximately $606M. A1643:6-16.

The jury heard other evidence valuing VirnetX's patents. Apple's corporate representative testified that Apple's alleged noninfringing alternative of relaying 100% of FaceTime calls could cost up to $720M. A1789:10-1795:10. Further, Apple's damages expert, Dr. Christopher Vellturo, agreed with Weinstein that the smallest salable unit for Mac computers was the $29 software upgrade. A2284:20-2285:2. Also, Vellturo used VirnetX's $200M limited-scope Microsoft license as his "benchmark" in determining his stacked royalty rate. A2258:6-18; A2290:7-2291:5.

After a five-day trial, the jury found all asserted patents infringed and awarded damages of $368,160,000—less than VirnetX sought, but more than Apple proposed. A240-41.

V. SUMMARY OF ARGUMENT

Apple attempts to turn the jury's factual findings and judge's evidentiary rulings into legal issues, notwithstanding the proper standard of review. When Apple does acknowledge the proper standard, it ignores contradictory evidence and pronounces its evidence "undisputed."

Though VirnetX presented substantial evidence through fact and expert witnesses and documents, Apple argues "undisputed evidence" shows its products cannot infringe. Calling its own documents unreliable and VirnetX's witnesses not credible, Apple contends (1) VPN On Demand does not perform a "determination"

nor initiate a VPN, secure channel, or encrypted channel "between" a client and target computer; and (2) FaceTime does not establish a "secure communication link." Because the jury was entitled to rely on Apple's documents and this Court may not reassess witness credibility, however, Apple has failed to show any error in the district court's denial of JMOL of infringement.

Apple's two claim construction arguments relate to FaceTime products. Both arguments would require this Court to read in elements from the specification and other claims. Nothing supports such limiting constructions. Under the district court's proper constructions, Apple acknowledges FaceTime meets the "domain name" requirement, and substantial evidence shows FaceTime establishes a "secure communication link."

Regarding invalidity, Apple contends "no reasonable jury" could have disagreed with its contention that Kiuchi anticipates. In so arguing, Apple selectively ignores Kiuchi itself, VirnetX's expert's testimony, and admissions by its own expert. The jury was entitled to consider this evidence and find the patents not invalid.

Apple advocates for a new trial, arguing the district court's exclusion of non-final reexamination evidence was "legally erroneous." Apple's case cites fail to support its proposition, and the court properly found the evidence more prejudicial than probative because it could improperly influence the jury regarding validity.

Three separate, properly admitted theories support the jury's damages award. Attempting to cast doubt, Apple mischaracterizes VirnetX's theories, ignores evidence, and argues evidentiary-weight issues under the guise of admissibility. Apple also wrongly claims Chief Judge Davis created a "new" theory. But Judge Davis's jury instruction merely captures that the entire market value rule *is the exception* to basing royalties on the smallest salable patent-practicing unit. That Apple disagrees with what constitutes the smallest salable unit does not change the rule of law. Nor does it undermine the substantial evidence supporting the proposed royalty base. Judge Davis also properly exercised discretion when admitting related licenses and two alternative theories directly tied to the invention's value.

VI. ARGUMENT

A. Standard of Review

VirnetX agrees with Apple's stated standards of review except as noted here. A district court's admission/exclusion of evidence under Fed. R. Evid. 403 is reviewed under regional circuit law. *Bose Corp. v. JBL, Inc.*, 274 F.3d 1354, 1360 (Fed. Cir. 2001). In the Fifth Circuit, such decisions should be affirmed "absent a clear abuse of discretion," resulting in "substantial prejudice." *Wellogix, Inc. v. Accenture, L.L.P.*, 716 F.3d 867, 882 (5th Cir. 2013).

B. The District Court Properly Denied JMOL of Noninfringement of the '135 and '151 Patents

1. Substantial Evidence Shows VPN On Demand "Determines Whether" a Secure Site Is Requested

Apple never sought construction of the "determining" step. And Apple acknowledged that "determining" does not require verification. A10175:11-12("And nobody is arguing—we are not arguing that there somehow requires some verification."). Accordingly, the jury was entitled to apply the ordinary meaning and find that VPN On Demand performs the determination just like the preferred embodiment of the '135 and '151 patents: by comparing the domain name in the domain name service request against a list of domain names. As noted *supra* 7-8, the specifications disclose that whether access to a secure site has been requested is determined "*by reference to an internal table of such sites*." A298(38:25-28)(emphasis added). It is undisputed that Apple's VPN On Demand products operate the same way. *See supra* 16-19.

Apple nonetheless argues there exists "undisputed evidence" that VPN On Demand does not "determine whether" because a user may misconfigure VPN On Demand, causing it to determine that a public website is a secure one—and consequently initiate a VPN because there was no verification the website was, in fact, secure. B.Br.25-26. But Apple's expert admitted inclusion of a public site in the configuration list would be "atypical" (A1992:5-1993:1) and, as this Court has

repeatedly held, whether VPN On Demand can be used in an unintended or unusual manner is legally irrelevant to infringement. *See Hilgraeve Corp. v. Symantec Corp.*, 265 F.3d 1336, 1343 (Fed. Cir. 2001); *z4 Techs., Inc. v. Microsoft Corp.*, 507 F.3d 1340, 1350 (Fed. Cir. 2007)("[I]nfringement is not avoided merely because a non-infringing mode of operation is possible.").

Apple's internal technical design documents, emails, and marketing presentations, as well as Jones's testimony, all support that VPN On Demand is *intended* for accessing secure private networks such as corporate networks—not public networks. *See supra* 17-19, 22-23. Not only do Apple's documents teach that VPN On Demand will "[d]etermine if the host is in the private network," but they explain that only private addresses should trigger a VPN. A15238; A15250; A15255; *see* A15236; A15055; A15490; A20017; A20001-03. Apple suggests these documents are mere "marketing documents" not accurately describing VPN On Demand's operation. B.Br.27-28. But Apple's own engineer agreed with the documents. A1406:7-19(Ridenour). Further, contrary to Apple's contention, the documents include design documents, technical presentations, and emails. In any event, it is entirely appropriate to rely on Apple's documents (marketing or otherwise) as "strong circumstantial evidence" of how their product was designed and intended to be used. *See Arthrocare Corp. v. Smith & Nephew, Inc.*, 406 F.3d 1365, 1377 (Fed. Cir. 2005).

Finally, Apple incorrectly asserts that the court relied on a new construction of "determining" post-verdict. B.Br.26-27. The court did nothing more than repeat what Apple earlier acknowledged: "determining" does not require verification. A40-41. It is Apple that now offers a new construction, contrary to its earlier statements (A10175:11-12), and requires "determining" to not only identify whether a request is for a secure website, but to verify that, in fact, the website is secure (B.Br.26-27). Apple's belated attempt to construe the term—after representing the opposite to the court—should be rejected. *Conoco, Inc. v. Energy & Envtl. Int'l, L.C.*, 460 F.3d 1349, 1359 (Fed. Cir. 2006)(finding waiver of construction first pursued post-trial). In any event, Apple's new construction should be rejected because it excludes a preferred embodiment—determining whether access to a secure site is requested by checking an internal list of sites. *On-Line Techs., Inc. v. Bodenseewerk Perkin-Elmer GmbH*, 386 F.3d 1133, 1138 (Fed. Cir. 2004)("claim interpretation that excludes a preferred embodiment" is "rarely, if ever, correct").

2. Substantial Evidence Shows VPN On Demand Performs the "VPN," "Secure Channel," and "Encrypted Channel" Elements

a. VPN On Demand Initiates a VPN and Secure Channel

VPN On Demand undisputedly encrypts traffic such that it is both secure and anonymous on the insecure path between the client and VPN server.

A1400:18-1401:11(Jones); A1998:1-6(Kelly). Further, as Jones testified, skilled artisans would understand that the path behind the VPN server and within the private network to the target computer is also secure and anonymous due to the physical security provided by the VPN server and private network. A1396:19-1398:11; A1401:12-18. As Jones explained, in his experience, companies configure private networks "to be secure." A1379:9-14; A1400:18-1401:18. The jury was entitled to credit Jones's testimony. Apple's reliance on expert testimony that traffic could be unsecured behind the VPN server in an "atypical" situation—when the configuration list includes a public website (B.Br.30 n.6; A1997:2-22)—does not address VPN On Demand's intended use (*supra* 35-36).

Apple also asks this Court to reweigh Jones's testimony and credibility, asserting his testimony rests on mere assumptions about how private networks operate. But Jones, an undisputed expert in the field of computer networks and network security (A1305:25-1309:22), testified based on his understanding and experience with private networks. *See LNP Eng'g Plastics, Inc. v. Miller Waste Mills, Inc.*, 275 F.3d 1347, 1361 (Fed. Cir. 2001)(reassessing witness credibility on appeal inappropriate). He also relied on Apple's internal technical presentations, product specifications, and marketing presentations (A1379:15-1383:13; A1394:17-1398:11; A1402:15-1407:9), which describe the security measures used by the private/corporate networks to which VPN On Demand is intended to

connect, including use of VPN servers, VPN authentication servers, proxy servers, and/or firewalls, before permitting access into or out of a private network. *Supra* 17-19, 22-23. The jury was entitled to rely on Jones's testimony and Apple's documents, which recognize communications within private networks are secure from and anonymous to unauthorized users outside the network.

The '135 and '151 patents also disclose that private networks (referred to in the specification as "LANs") are commonly secured by firewalls. A280(2:51-54("[f]irewalls attempt to protect LANs from unauthorized access")); A385(53:58-61). Though the patents caution that firewalls cannot always protect private networks against hostile *authorized* users, VPN On Demand is intended to access secure networks (*supra* 35-36), which are intended to be secure against *unauthorized* users. A280(2:57-60); A385(53:58-61).

Apple's contention that Jones and Short (an inventor) "conceded" that private networks are not secure or anonymous is plainly wrong. B.Br.31-32. Jones's alleged "concession" is a simple statement that traffic within private networks need not be *encrypted* (A1379:9-14), consistent with "VPN's" construction that *insecure* paths be encrypted. But, as the patents state and the district court correctly recognized, there are a "tremendous variety of methods" to provide security and anonymity, and "encryption is not the only means of addressing data security." A280(1:15-17); A13.

As for Short, he merely admitted private networks may not be secure from *authorized* hostile employees (A1164:12-22), and that sometimes mistakes are made and a private network is not actually secure (A1160:24-1161:13). He also testified that a private network "is secure, because it's been physically secured; and" has a "firewall between its network and the public network. So it keeps the bad guys out." A1080:4-15. At most, Short's testimony reveals private networks are intended to provide security and anonymity, and do so except under unusual conditions. But there is no requirement a "VPN" or "secure channel" be *invincibly* secure. Further, as noted above, operation of an accused device in an unusual manner is legally irrelevant to infringement. *See Hilgraeve*, 265 F.3d at 1343. Substantial evidence demonstrates communication within a physically secured LAN satisfies the "VPN" and "secure channel" requirements and, accordingly, supports the jury verdict.

b. VPN On Demand Initiates an Encrypted Channel Under the Doctrine of Equivalents

Turning to '151 patent claim 1, Apple disputes whether substantial evidence supports the jury verdict of equivalent infringement. B.Br.32. But the issue before the jury was not whether an unencrypted channel is equivalent to an encrypted channel, as Apple argues. B.Br.33. Rather, it was whether a channel, which is encrypted on the physically unsecured portion and potentially unencrypted on the

physically secured portion, is equivalent to an "encrypted channel." It is, and substantial evidence supports that conclusion. *See supra* 23-24.

Jones testified that the difference between secure communication in a private network and secure communication via encryption is insubstantial. A1421:9-24. He explained, in detail, how VPN On Demand satisfies the function-way-result test. He explained VPN On Demand performs substantially the same function as an encrypted channel by securing communication between the client and secure server either through encryption or the protection offered by a private network. A1424:4-14; *see also* A1378:23-1379:14; A1400:18-1401:18. He also explained VPN On Demand performs in substantially the same way as an encrypted channel by protecting data through encryption on paths vulnerable to eavesdroppers, i.e., insecure paths. A1424:15-20; *see also* A1392:9-18; A1400:18-1401:18. Lastly, he explained how Apple's products achieve substantially the same result as an encrypted channel by protecting communication from potential eavesdroppers. A1424:21-25; *see also* A1392:9-18; A1400:18-1401:18. The jury was entitled to credit this testimony.

As set forth above and *supra* 23-24, Jones's analysis was far from "perfunctory," as Apple asserts. B.Br.33. Rather, he incorporated his earlier testimony regarding secure communications and provided his rationale—"'the

particularized testimony and linking argument' necessary to prove equivalence" (B.Br.33)—supporting his conclusion of equivalence.

C. The District Court Properly Denied JMOL of Noninfringement of the '504 and '211 Patent Claims

1. The District Court Properly Construed "Domain Name"

a. The Intrinsic Evidence Supports the District Court's Construction

The intrinsic evidence fully supports the court's broader construction of "domain name" as "a name corresponding to an IP address." As the specification makes clear, the inventions use domain names for purposes well beyond retrieving web pages on the Internet through standard DNS. Specifically, the specification teaches the use of domain names to secure communications for "video conferencing, e-mail, word processing programs, telephony, and the like" (A369(21:27-29)), which use telephone numbers or email addresses corresponding to an IP address instead of "web.com." That the inventors used the word "domain name" in a broader sense is further supported by the specification's reference to "non-standard top-level domain name," "non-standard domain name," "top-level domain name," and "standard top-level domain name." A383(49:29, 50:36-38). The use of different adjectives to further modify "domain name" shows that the inventors did not intend to limit "domain name" to a particular format ("standard," "top-level," or otherwise), but rather they defined this term by the important function it serves: corresponding to an IP address.

Consistent with this, VirnetX's expert testified that, after reading the patents, skilled artisans would understand the ordinary meaning of "domain name" as "a name corresponding to an IP address" and would not restrict it to a "hierarchical sequence of words." A6083-84; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1321 (Fed. Cir. 2005)("'[O]rdinary meaning' of a claim term is its meaning to the ordinary artisan after reading the entire patent."). As VirnetX's expert explained, the use of hierarchical domain names is useful on the Internet to provide distributed management of domain name look-up, but unnecessary for the other smaller networks discussed and claimed in the patents, which need not return IP addresses corresponding to every possible domain name on the Internet. A6083-84(¶10). Indeed, the patents contemplate "'boutique' embodiments" that are "robust for use in smaller networks, such as small virtual private networks" (A366(16:36-38)), as well as video conferencing, email, and telephony embodiments (A369(21:27-29)).

Furthermore, the claims themselves indicate the "domain name" corresponds to an IP address. '504 patent claim 1 and '211 patent claim 36 recite storing "a plurality of domain names and corresponding network addresses." Additionally, claim differentiation undermines Apple's attempt to confine "domain name" to a particular hierarchical structure with the format: (i) a top-level domain; (ii) a second-level domain; and (iii) a host-name. B.Br.34-35. Dependent claim 2 of the '504 patent and dependent claim 37 of the '211 patent both require the plurality of

domain names to include "*at least one* top-level domain name." Accordingly, both the independent and dependent claims contemplate and include domain names *without* such a hierarchical format. "The doctrine of claim differentiation is at its strongest in this type of case, 'where the limitation that is sought to be 'read into' an independent claim already appears in a dependent claim.'" *InterDigital Commc'ns, LLC v. ITC*, 690 F.3d 1318, 1324 (Fed. Cir. 2012).

Apple's reliance on exemplary domain names like "Yahoo.com" in the specification is misplaced. B.Br.35. As the court noted, these are simply "examples" and nothing in the specification limits the invention to them. A5488; A16. As such, these examples cannot "be used to rewrite[] the chosen claim language." *SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004).

The court's construction is also supported by VirnetX's statement during prosecution of the related '181 patent that a domain name may encompass a "telephone number." A20836. In a later reexamination requested by Apple, both the Examiner and Apple cite this statement to interpret the claims. A20846; A20879; A20881; A20888; A20890.

b. Apple's Extrinsic Evidence Cannot Overcome the Intrinsic Evidence

Apple argues that the court, in incorporating portions of its *Markman* ruling from *Microsoft*, unfairly penalized Apple for Microsoft's reliance on extrinsic

evidence. B.Br.36 n.8. But Apple's attempts to confine "domain name" were not appreciably different from Microsoft's. Both Apple and Microsoft relied heavily on extrinsic evidence for the alleged "ordinary meaning" of "domain name." B.Br.34-35. In particular, Apple relies on a technical dictionary and a description of the Internet in an unrelated case before this Court. *Id*. Neither can trump the language of the claims or the specification.

Apple first cites a 1997 dictionary defining "domain name" as having a "hierarchical format." B.Br.34. The full definition, not quoted by Apple, reveals the definition is limited to web pages on the Internet. A6140. The patents are not so limited. *See supra* 9, 42-44. Apple next cites an unrelated case, in which this Court described the organization of web pages on the Internet. B.Br.34-35. But, the Court's "background" discussion there did not construe "domain name" as a matter of law for all cases and all patents.

Finally, Apple contends VirnetX "conceded" that domain names have a hierarchical syntax. B.Br.35. This is not so. Instead, VirnetX explained that while domain names for large networks such as the Internet typically have a hierarchical organization, the patents are not so limited. A7138-39.

Apple likewise asserts that VirnetX's expert (Jones) admitted a phone might not have a domain name. B.Br.34. But his statement, made in response to Cisco's limited construction of "domain name" in *Microsoft*, referred only to a particular

type of domain name restricted to web pages on the Internet. A7093. As discussed above, the patents are not so limited. Because the specification considers networks beyond mere web pages, skilled artisans would understand phone numbers and email addresses can constitute domain names. A1325:13-20; A1460:9-19; A6083-84(¶10).

2. Even Under Apple's Construction, Disputed Issues of Fact Would Remain

This Court should affirm the district court's construction and the jury's verdict. But, if the Court were to adopt Apple's construction, it should remand for resolution of disputed facts. *See Electro Scientific Indus., Inc. v. Dynamic Details Inc.*, 307 F.3d 1343, 1350 (Fed. Cir. 2002). Given the district court's construction, it was unnecessary for VirnetX to introduce evidence that email addresses, with their top-level domain names such as ".com," and phone numbers, organized by area code, have hierarchical formats. And Apple introduced no evidence that they do not meet its construction of "domain name."

3. The District Court Properly Construed "Secure Communication Link"

a. Apple Waived Its Construction Argument

Apple successfully pursued its construction of "secure communication link" as a direct link requiring encryption before the district court (A7992; *see supra* 26) and is now precluded from pursuing a different construction. *See Digital-Vending Servs. Int'l, LLC v. Univ. of Phoenix, Inc.*, 672 F.3d 1270, 1278 (Fed. Cir.

2012)(party waives new construction after lower court adopts parties' agreed construction).

b. Intrinsic Evidence Supports the District Court's Construction

In any event, the '504 and '211 patent claims broadly recite a "secure communication link"—not VPN. "Had the inventors intended [the VPN] limitation, they could have drafted the claims to expressly include it." *i4i Ltd. P'ship v. Microsoft Corp.*, 598 F.3d 831, 843 (Fed. Cir. 2010), *aff'd*, 131 S. Ct. 2238 (2011). Indeed, in a related patent, the claims expressly recite "the secure communication link being a virtual private network communication link." A6592(57:20-22, 58:32-34). Additionally, dependent claims in the '504 and '211 patents indicate "the virtual private network *is one of* a plurality of secure communication links." A386(56:8-10(emphasis added)); A527(55:65-67).

The specification echoes this point, using "secure communication link" or "path" more generically than VPN and recognizing the difference between secure communication paths and anonymous paths. For example, in describing a conventional architecture, the specification uses the term "secure communication path" even when "the true IP address of that web site would be revealed over the Internet," and thus the path is not anonymous. A378(39:24-33). The specification also uses the terms "VPN communication link" and "secure communication link" to mean different things, indicating that, "[a]ccording to one variation of the

invention," a VPN communication link is a *type* of secure communication link. A383(49:31-45). This particular embodiment of the VPN link, unlike the secure communication link, provides anonymity via an "address hopping regime" or other techniques. A383-84(50:60-51:7, 51:62-52:2).

Thus, the specification discloses that data security and anonymity are two *separate* requirements that may, but need not, be addressed together. Referring to data security, the specification explains, "[i]t is desired for the communications to be secure, that is, immune to eavesdropping." A359(1:40-41). With respect to anonymity, the specification explains, "[a]lso, it *may* be desired to prevent an eavesdropper from discovering that terminal 100 is in communication with terminal 110." *Id.*(1:43-52)(emphasis added). Contrary to Apple's assertion that both are always required (B.Br.38-40), the specification explicitly teaches that different users have "different needs" and, in some instances, data security may be desired, whereas in others, anonymity may *also* be desired (A359(1:33-52)).

Apple next asserts that "every" disclosed embodiment discusses secure and anonymous communications, but Apple *only* points to embodiments employing a "two-layer encryption" scheme referred to as the "TARP" VPN protocol. B.Br.13, 39-40. In describing TARP VPN, the term "secure communication link" is never used. *See, e.g.*, A363-68(9:41-20:11). Nor are these embodiments recited in the

asserted claims. Where related embodiments potentially involving TARP VPN are recited, the claims explicitly require a VPN link. *See, e.g.*, A386(56:11-26).

c. Misplaced Reliance on the ’181 Patent

Apple’s reliance on the ’181 patent specification and prosecution history (B.Br.40-41) is misplaced. Like the ’504 and ’211 patents, the ’181 patent discloses a generic embodiment for establishing a secure communication link. A6821(48:53-55.) The patent then discloses that, “[a]ccording to one variation of the invention,” a user may select a VPN link, which in that particular embodiment provides anonymity. A6822(49:19-27, 50:42-56). It is in this context, namely, the alternative embodiment, that the patent specifies “anytime that a communication link is established, the link is a VPN link.” A6823(51:67-52:1). Any alleged “equating” of a “secure communication link” with a VPN link in the abstract and specification (B.Br.40) refers to preferred embodiments. A6800-01(6:32-7:6(“one aspect of the present invention” and “[i]n one embodiment”)).

Apple next contends the prosecution history of the ’181 patent indicates a “secure communication link” must be a VPN link because it mentions private networks. B.Br.40-41. Apple is wrong. A secure communication link may connect to a device in a private network; the presence of a private network does not automatically necessitate a VPN link. *See* A1323:23-1324:6. At most, VirnetX’s statements during prosecution indicate a secure communication link should be

direct. *See supra* 11-12. Nothing in VirnetX's statements evidences a "clear and unmistakable" disavowal that a *secure* communication link cannot simply be secure, but must be secure *and anonymous* or a VPN. *Cordis Corp. v. Medtronic AVE, Inc.*, 511 F.3d 1157, 1176-77 (Fed. Cir. 2008)(argument-based disavowals require "clear and unmistakable surrenders of subject matter").

d. If This Court Adopts Apple's Construction, Disputed Issues of Fact Remain

If the Court were to agree with Apple's construction, it should remand for resolution of disputed facts. *See Electro Scientific*, 307 F.3d at 1350. Contrary to Apple's allegations, Jones did not introduce evidence that FaceTime communications are not anonymous. B.Br.41-42. In fact, as Apple recognized, Jones testified that FaceTime communication is sent via "encrypted packets." *Id.*; A1465:17-20. That some types of messages may not be encrypted or that NAT routers may identify a particular device does not necessarily defeat anonymity as it pertains to potential eavesdroppers. Neither Apple nor VirnetX introduced evidence that FaceTime communication is not anonymous.

4. Substantial Evidence Shows FaceTime "Supports Establishing a Secure Communication Link"

As Apple advocated, the district court construed "secure communication link" to require direct communication. A13. Under that construction, the jury was

entitled to rely on Jones's testimony and Apple's documents, and find that FaceTime communication via NAT routers constitutes direct communication.

The court acknowledged Apple argued "direct" means "direct addressability," and nonetheless concluded that "routers, firewalls, and similar servers that participate in typical network communication do not impede 'direct' communication between a client and target computer." A8 n.2. Apple has never disagreed with this conclusion. A2656:13-2659:4. Moreover, substantial evidence reveals NAT routers are a type of router that does not impede direct communication. *Supra* 20-22, 27. Indeed, Jones testified FaceTime communication occurs via UDP, a transport layer protocol, that is direct and uninterrupted between FaceTime devices. A1465:8-20(Jones). And Apple's expert likewise admitted NAT routers do not stop or terminate communication between FaceTime devices. A1984:10-19(Kelly). As Apple explained, NAT routers are typically used in network communication between public spaces such as the Internet and private spaces like a home. A1043:5-14(Apple Opening Statement); A1785:22-1786:5(Gates).

The jury further heard from Jones that NATs merely translate a transport address, which identifies a target device, from the public address space to the private address space. A1467:16-25; A1536:10-25. Apple conceded as much. B.Br.42; A1969:21-1970:2(Kelly); A2658:2-4. Thus, as Jones testified, NAT

routers allow for direct addressability by simply translating addresses mapped to particular devices and not, as Apple contends, readdressing communications.

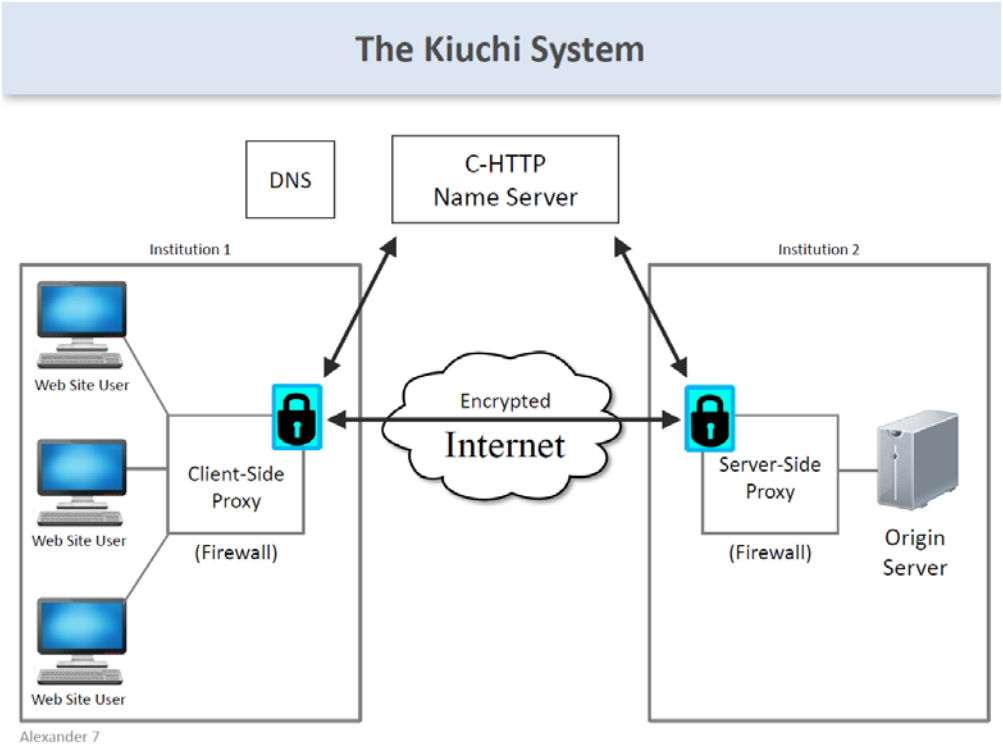
Apple's internal technical presentations, specifications, and emails support Jones's testimony, explaining that NAT routers "[c]reate[] direct peer-to-peer connections." A15394; A15449; A15479; A15485. Nevertheless, Apple argues that its documents cannot be trusted, and the court and jury erred in relying on them. B.Br.45. Apple further argues, without explanation, that the "direct *connections*" discussed in its documents are somehow different from direct *communications*. B.Br.45. Nothing in Apple's documents supports such a distinction, and Apple itself uses these terms interchangeably. *See, e.g.*, B.Br.20, 29. Apple's attempts to distance itself from its documents must be rejected.

Lastly, Apple argues that the court's finding that NAT routers do not impede direct communication conflicts with VirnetX's statements during prosecution that direct communication involves data "addressed to a target." B.Br.44-45. But, as explained above and *supra* 20-22, FaceTime communication via NAT routers *does* address the target—specifically, the target's transport address. Thus, the jury was entitled to find that FaceTime communication via NATs is direct.

D. The District Court Properly Refused to Overturn the Jury's Findings that the Patents Are Not Invalid

1. Substantial Evidence Supports that Kiuchi Does Not Anticipate the '135 Patent

Substantial evidence supports that Kiuchi does not anticipate the claims. Jones testified that the client-side and server-side proxy servers in Kiuchi, shown below, do not allow for direct communication between a client and target computer, as required by the '135 patent claims. A2343:14-2344:7; *see supra* 27-28.



Specifically, Jones explained, at length, that the proxy servers are terminating servers that stop communication, process the data, and then initiate another connection or communication. A2334:25-2335:11; A15009-10. In this way, the

Kiuchi proxy servers impede direct communication just like Apple stated the proxy servers in Aventail do. *See* A2661:6-17; A2710:3-6. Apple's expert, Alexander, agreed that the proxy servers in Kiuchi do indeed process the message before sending it on. A2200:18-2201:3. And Kiuchi itself explains the proxy servers stop communication between the client—shown as the Web Site User—and the origin server, extract the message, encrypt/decrypt the contents, rewrite the message, and establish a new communication. A15009-10. Accordingly, the judgment should be affirmed.

2. Substantial Evidence Supports that Kiuchi Does Not Anticipate the '151 Patent

Apple asserts that Kiuchi anticipates the '151 patent claims by reading the "client-side proxy" in Kiuchi (see figure above) on the claimed "client." B.Br.47-48. But Kiuchi teaches that the "client" is the "website user"—not the proxy—and Alexander agreed this was the "natural read" of the reference. *See supra* 27. This reason alone supports affirmance.

3. Substantial Evidence Supports that Kiuchi Does Not Anticipate the '504 and '211 Patents

As with the '135 patent, Apple alleges Kiuchi discloses direct communication between the client and origin server to satisfy the "secure communication link" requirement in the '504 and '211 patent claims. B.Br.48.

But, as discussed above, the jury heard substantial evidence that the proxy servers prevent direct communication. *See supra* 27-28, 53-54.

Apple next argues the jury was not free to disbelieve its argument that Kiuchi inherently teaches storing "a plurality of domain names and corresponding addresses" because registration of the server-side proxy "necessarily" involves storing its IP address and domain name. B.Br.48. But, as the jury heard, Kiuchi expressly teaches that registration of the server-side proxy involves the IP address alone. A15009("register an IP address (for a server-side proxy . . .)"); *see* A2378:1-9. Apple also misleadingly contends Jones testified Kiuchi was not enabling merely because of an incorrect appendix. B.Br.49. Rather, he explained that, notwithstanding an incorrect appendix, Kiuchi's text correctly teaches the C-HTTP name server stores names of *origin servers*—not the server-side proxies—and IP addresses of *server-side proxies*. A2336:20-2338:20; A15009; *see supra* 28. Since IP addresses of server-side proxies do not "correspond" to origin servers, and neither Kiuchi's appendix nor text teaches otherwise, this limitation is not met. Accordingly, substantial evidence supports the jury's finding of no anticipation.

E. The District Court Did Not Abuse Its Discretion Excluding Evidence of Ongoing Reexaminations

Citing *Commil USA, LLC v. Cisco Systems, Inc.*, 720 F.3d 1361, 1368 (Fed. Cir. 2013), for the position that a good-faith belief of invalidity may negate

the requisite intent for induced infringement, Apple argues evidence of non-final reexaminations demonstrates good-faith belief of invalidity and should have been admitted. B.Br.49-50. But this Court previously addressed the issue of reexamination evidence as it applies to invalidity, finding it has little probative value and "does not establish a likelihood of patent invalidity." *Hoechst Celanese Corp. v. BP Chems. Ltd.*, 78 F.3d 1575, 1584 (Fed. Cir. 1996); *see also Acoustical Design, Inc. v. Control Elecs. Co.*, 932 F.2d 939, 942 (Fed. Cir. 1991)(finding reexamination proceeding rejections "hardly justif[y] a good faith belief in the invalidity of the claims," especially where claims are eventually confirmed).

In *Commil*, invalidity was tried separately from induced infringement and the Defendant, Cisco, was prevented from introducing invalidity and induced infringement evidence together, effectively precluding it from showing good-faith belief of invalidity. 720 F.3d at 1365, 1367. Cisco argued it should have been allowed to introduce evidence of obviousness, anticipation, lack of written description, and enablement. *See* Brief for Defendant-Appellant Cisco Systems, Inc. at 20-21, *Commil*, 720 F.3d 1361 (No. 2012-1042), 2012 WL 830381, at *16. Notably, Cisco did not argue it should have been allowed to submit reexamination evidence. *See id.* Moreover, unlike Cisco, here, Apple submitted invalidity evidence, including the type Cisco was prevented from introducing in *Commil*. *See, e.g.*, A2028:14-2131:1; A2207:6-2226:16; A2233:19-2237:13; A15001-20.

Apple cannot demonstrate any prejudice from excluding reexaminations—nothing stopped Apple from presenting the merits of the invalidity theories under consideration in reexamination. Instead, Apple presented just one invalidity theory, which the jury rejected. Even assuming reexamination evidence is probative of a good-faith belief of invalidity, this probative value is far outweighed by potential prejudicial effect. *See SynQor, Inc. v. Artesyn Techs., Inc.*, 709 F.3d 1365, 1380 (Fed. Cir. 2013)(no abuse of discretion excluding non-final reexamination evidence because it "would have been confusing and more prejudicial than probative"). This Court has affirmed an exclusion even where final office actions were entered and on appeal, holding that "the prejudicial nature of evidence concerning the ongoing parallel re-examination proceeding outweighed whatever marginal probative or corrective value it might have had in this case." *See Calloway Golf Co. v. Acushnet Co.*, 576 F.3d 1331, 1343 (Fed. Cir. 2009); Brief of Defendant-Appellant Acushnet Company at xv, Calloway, 576 F.3d 1331 (No. 2009-1076), 2009 WL 434213, at *9(discussing reexaminations' status). Here, the court determined Apple's reexamination evidence was "highly prejudicial evidence that risks misleading the jury." A67. Its introduction "could have improperly influenced the jury's decision regarding validity." *Id.* (citing *Callaway*, 576 F.3d at 1342). The court did not abuse its discretion.

F. The Court Should Affirm the Damages Award

1. The Jury Instruction Was Correct: There Is No Per Se Rule that an Entire Product Cannot Constitute the Smallest Salable Patent-Practicing Unit

Judge Davis's jury instruction correctly accounted for the fact that the "entire market value rule is a narrow exception to the general rule that royalties are awarded based on the smallest salable patent-practicing unit." *Versata Software, Inc. v. SAP Am., Inc.*, 717 F.3d 1255, 1268 (Fed. Cir. 2013)(citing *LaserDynamics, Inc. v. Quanta Computer, Inc.*, 694 F.3d 51, 67 (Fed. Cir. 2012)). If the smallest salable unit is used, "the award cannot violate the entire market value rule." *Id.*

By definition, the entire market value rule exception only applies when the "entire market value" of the accused products is used, not when the revenue is properly apportioned. *See Garretson v. Clark*, 111 U.S. 120, 121 (1884). As exemplified in *LaserDynamics* and *Cornell*, the apportionment requirement does not mean the smallest salable unit cannot contain unclaimed features or constitute entire products. In *LaserDynamics*, the smallest salable unit was an optical disk drive that practiced the claimed method, contained unclaimed features, and was an entire product sold separately. 694 F.3d at 56, 58-59, 69-70, 78-79. Similarly, in *Cornell*, the invention was but "a small part" of a portion of the processor, yet the processor—sold separately—constituted the smallest salable unit. *Cornell Univ. v. Hewlett-Packard Co.*, 609 F. Supp. 2d 279, 283-84, 288 (N.D.N.Y.), *amended*,

No. 01-CV-1974, 2009 WL 1405208 (N.D.N.Y. May 15, 2009)(Rader, C.J., sitting by designation). Although a small royalty rate cannot overcome an improper royalty base, the rate necessarily reflects the invention's contribution to the proper royalty base.

In seeking to fault the jury instruction, Apple essentially argues for a new per se rule that an entire product cannot constitute the smallest salable unit. This Court should reject that outright. The Supreme Court and this Court have cautioned against per se rules in fact-intensive and case-specific inquiries like damages. *See, e.g.*, *Sprint/United Mgmt. Co. v. Mendelsohn*, 552 U.S. 379, 387 (2008)(critiquing "broad *per se* rules"). What constitutes the smallest salable unit in a particular case is best left for the jury. Here, both parties presented evidence and argument on the smallest salable unit—which, with respect to some products, was undisputed—and the jury was entitled to weigh that evidence in determining the award. *Supra* 16, 19-20, 29-30; *infra* 60-62.

Apple's contention that *Lucent* and *Uniloc* would have been wrongly decided under the jury instruction is incorrect. B.Br.53. Those cases did not address the smallest salable unit, and there was no attempt to apportion the royalty base as was done here. For these same reasons, the instruction is not inconsistent with *Garretson*, *Rite-Hite*, and *Uniloc*. In these cases, the royalty base consisted of the *entire* market value of the products without apportionment. In *Rite-Hite*, for

example, the damages base included sales of *separate* components sold together for marketing reasons—a far cry from the smallest salable unit. *See Rite-Hite Corp. v. Kelley Co.*, 56 F.3d 1538, 1550-51 (Fed. Cir. 1995). Because the jury instruction was in line with precedent, it provides no basis to alter the verdict.

2. Substantial Evidence Supports that the Royalty Base Only Included the Smallest Salable Patent-Practicing Units

Apple next argues VirnetX's royalty base was legally unjustified. B.Br.56. But VirnetX's proposed royalty base did not include the entire market value of the accused products (a figure never presented to the jury). For Macs, both experts agreed the smallest salable unit was the $29 software upgrade. A1619:15-22; A2284:20-2285:2. Weinstein reasonably explained, however, even in the face of vigorous cross-examination, that the Mac software upgrade price was not the smallest salable unit for iOS devices; indeed, they cannot be upgraded with software to add FaceTime because they lack necessary hardware (i.e., front-facing camera). *E.g.*, A1619:15-21; A1674:8-16; A1719:18-1720:9; *see also* A2325:24-2326:6. And, for Apple's iOS devices, software creates the largest share of the product's value, showing further that the $29 software upgrade would be inappropriate for iOS devices. *See* A2321:4-22; A2324:2-25. Thus, as Weinstein explained to the jury, he used the smallest salable unit, apportioning out every feature possible and using the lowest price at which each model was ever sold. A1616:10-20; A1618:22-1619:22; A1620:11-22; *see also supra* 16, 19-20, 29-30.

The jury was entitled to credit this testimony. Indeed, calculating a reasonable royalty "necessarily involves an element of approximation, and uncertainty," *i4i*, 598 F.3d at 857-58, and there are "several approaches," *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301, 1324 (Fed. Cir. 2009). In any approach, "[q]uestions about what facts are most relevant or reliable to calculating a reasonable royalty are for the jury." *See i4i*, 598 F.3d at 856. Further, the reasonable royalty may reflect that "an infringer had to be ordered by a court to pay damages, rather than agreeing to a reasonable royalty." *Maxwell v. J. Baker, Inc.*, 86 F.3d 1098, 1109-10 (Fed. Cir. 1996). Contrary to Apple's assertion (B.Br.59-60), it is commonplace to charge different royalties for different products, e.g., a Mac computer as compared to mobile devices, as shown by licenses presented to the jury. *See* A2306:23-2307:2; A2309:8-13; A20356-80; A20388-411; A20424-53. Apple also incorrectly asserts that Weinstein's $15 attribution per iOS device to FaceTime shows further apportionment is possible. B.Br.60. Not only does this not account for VPN On Demand, but it concerns a different, but acceptable, way of calculating a reasonable royalty. *Cf. Lucent*, 580 F.3d at 1324 ("several approaches for calculating a reasonable royalty" (citing *TWM Mfg. Co. v. Dura Corp.*, 789 F.2d 895, 899 (Fed. Cir. 1986))). Apple's reference to evidence that might have supported a different smallest salable unit does nothing to

show that substantial evidence does not support the jury's award.[4] *See TWM Mfg.*, 789 F.2d at 899 ("[Defendant's] pointing to facts that might have supported a lower royalty does not sustain its burden of showing" error.).

Moreover, the concerns exemplified in the entire-market-value-rule cases cited by Apple are not present here. B.Br.56-57. The rule, in effect, "acts as a check," ensuring the damages sought "are in fact 'reasonable' in light of the [invention]." *LaserDynamics*, 694 F.3d at 67. As explained, Weinstein accurately accounted for the invention's value through three separate theories and a thorough *Georgia-Pacific* analysis. Unlike in *Lucent*, Weinstein did not adjust his rate to obtain the same figure he would have using the entire market value. *See* 580 F.3d at 1338.

3. District Court Did Not Abuse Its Discretion Admitting Licenses

The court properly exercised its discretion admitting the licenses-at-issue. *See i4i*, 598 F.3d at 852 (citing *Huss v. Gayden*, 571 F.3d 442, 452 (5th Cir. 2009)). Apple made a tactical decision at trial to agree to not refer to the licenses as settlements (A10007(no.19); A10012; A1003:11-1004:14), not object to their admission (A1051:25-1052:19; A10013-36), and use one as a "benchmark."

[4] Apple fails to contest—and thus concedes—the smallest salable unit bore a "close relation" to the invention. *See, e.g.*, *Finjan, Inc. v. Secure Computing Corp.*, 626 F.3d 1197, 1207 (Fed. Cir. 2010).

Apple waived arguments otherwise. *See* Fed. R. Evid. 103. Nonetheless, each license is directly related to the patents-in-suit, and any differences with the hypothetical negotiation were thoroughly explained to the jury. Apple's arguments, at their core, go to weight, not admissibility. *See ActiveVideo Networks, Inc. v. Verizon Commc'ns, Inc.*, 694 F.3d 1312, 1333 (Fed. Cir. 2012)(citing *i4i*, 598 F.3d at 854).

Apple takes issue with the fact that the SAIC/In-Q-Tel agreement concerned technology leading to the invention and that the SAIC/SafeNet license covered pending applications (e.g., '135 patent's application) and involved software. B.Br.61-62; A20265; A1596:14-1598:10. These types of licenses, however, properly inform an expert's reasonable royalty analysis. *ActiveVideo*, 694 F.3d at 1333 (affirming admission of expert testimony on license not involving patents-in-suit or technology-at-issue and on agreement covering both "patents *and* software services"). "The degree of comparability" of the license agreements is a "factual issue[] best addressed by cross examination and not by exclusion." *Id.* (citing *i4i*, 598 F.3d at 852). The jury heard extensive testimony about the circumstances of these licenses, how they relate to the patents-in-suit, the parties to the licenses, the relevant terms, and how they inform the hypothetical negotiation. *E.g.*, A1084:13-1085:9; A1087:9-1089:8; A1094:22-1095:14; A1096:6-14; A1104:3-1107:5; A1116:12-21; A1176:14-1177:8(Short); A1192:9-1194:14(Munger); A1242:2-

22(Larsen); A1596:3-1598:10(Weinstein). This testimony included vigorous cross-examination and contrary testimony by Apple's expert (*e.g.*, A1134:22-1135:11; A1251:10-20; A1678:2-25; A2256:1-4)—the appropriate means of attacking this evidence. *See Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 596 (1993).

Apple's arguments concerning the Microsoft agreement (B.Br.62-63) are baffling considering Apple's own expert used this license "as a benchmark" for his royalty rate (A2258:6-12; A2263:20-25). *See Versata*, 717 F.3d at 1268 (defendant "cannot legitimately challenge the comparability of its own comparable."(citation omitted)). Differences between this license and the hypothetical negotiation were explained to the jury. *E.g.*, A1115:3-1116:8(Short); A1200:17-1201:4(Munger); A1233:4-1234:23; A1245:3-1246:14; A1271:17-1272:4(Larsen); A1599:6-1600:6; A1601:17-22(Weinstein); A20343-55; *see also* A1717:13-1718:17(discussing effective rate). For example, Larsen explained Microsoft received a "special deal" for a limited field-of-use license because it was the first licensee and VirnetX needed the money. A1245:3-1246:14. As in *Finjan*, "[t]hese differences permitted the jury to properly discount the Microsoft license." 626 F.3d at 1212.

Apple again failed to preserve any error regarding the admission of the Aastra, Mitel, and NEC licenses by not objecting to their admission. Moreover,

Apple's arguments concerning these licenses (B.Br.62) covering the patents-in-suit suffer from the same flaws—they go to the weight of the evidence. That these were three years after the hypothetical negotiation does not warrant their exclusion because they are part of the "book of wisdom that courts may not neglect." *Sinclair Ref. Co. v. Jenkins Petroleum Process Co.*, 289 U.S. 689, 698 (1933); *Lucent*, 580 F.3d at 1333. Rather, the difference in time, number of patents, and VirnetX's financial position go to the weight of the evidence, not its admissibility. *See ActiveVideo*, 694 F.3d at 1333. And, although these agreements were, at the time of trial, less than a million dollars, they cover sales of current and future products encompassing the licensed technology, such that they were projected to be worth millions. A1244:8-22; A1299:23-1300:13; A20357-58; A20389-90; A20425-26.

Apple does not contest the admissibility of the SAIC/VirnetX agreement in its opening brief—nor did it object to its admission at trial—waiving any such argument. *See, e.g.*, *Finjan*, 626 F.3d at 1207. Nonetheless, this agreement, like the others, was properly admitted because it concerns the patents-at-issue, and its relevance and differences were thoroughly explained. *See, e.g.*, A1116:22-25(Short); A1228:13-1229:20; A1294:21-1295:10(Larsen); A1598:11-1599:5(Weinstein).

Apple's perfunctory complaint about Weinstein's consideration of VirnetX's licensing policy should be rejected. B.Br.61 n.16. Weinstein's consideration of the policy in his *Georgia-Pacific* analysis was proper because it was the policy at the time and set out what VirnetX "hoped for," helping inform what VirnetX would have agreed to at the time—especially since the other licenses, except for the limited-scope Microsoft license, were in strict compliance. *See, e.g.*, A1595:6-19; A1602:4-16; A1613:21-1614:7; A1652:23-1653:6. Notably, Apple does not contest the policy's admission, nor did it object to Larsen's extensive discussion about the policy or other licenses. *See, e.g.*, A1228:13-1229:20; A1233:4-1234:15; A1238:3-1241:5; A1242:2-1247:12. Admitting this evidence was not an abuse of discretion.

4. Nash Bargaining Solution Analysis Is Directly Tied to the Facts of the Case and Properly Admitted

The focus of a Fed. R. Evid. 702 inquiry "must be solely on principles and methodology, not on the conclusions that they generate." *Daubert*, 509 U.S. at 595. Nobel prize winner, Dr. Nash, developed the Nash Bargaining Solution ("NBS"), which "has been applied extensively in different branches of economic theory." A20785(Nobel Prize website); *see, e.g.*, A20793("economic models of bargaining [(including NBS)] can be useful in understanding the hypothetical negotiation" in patent-damages cases). The theory builds on the *Georgia-Pacific*

analysis "by interpreting evidence and data in ways that reflect actual economic conditions affecting the outcome of the hypothetical negotiation." A20771.

NBS is in stark contrast to the 25% "rule of thumb" that assumed in every case an infringer would pay 25% of its *entire* profits of the infringing product. *See Uniloc USA, Inc. v. Microsoft Corp.*, 632 F.3d 1292, 1312 (Fed. Cir. 2011). NBS is case-specific and only divides *extra* profit that would not exist but for the invention's inclusion in the product. A1630:4-1633:10; A20772-73. Moreover, substantial evidence of numerous articles supporting the economic rigor of NBS were admitted without objection. *See* A20474-707; A20730-825.

An NBS analysis identifies the extra profit from including the technology in the product. Because the licensee would not agree to a deal worth less to it than employing a noninfringing alternative, the licensee is allocated the portion of this profit that could have been obtained using the noninfringing alternative. The same concept applies if the licensor has alternatives (e.g., product sales). After allocating profits from alternatives, the parties bargain over the remaining profit. If they have equal bargaining power and no other factors are present, they split the profit equally. *See* A1630:4-1633:10; A20772-73. Thus, NBS is directly tied to the facts of each case.

Apple does not assert noninfringing alternatives or other factors affecting the split beyond the parties' relative bargaining power. But, because Apple had more

bargaining power, Weinstein reduced VirnetX's share by 10%. A1633:11-17. Despite Apple's suggestion otherwise (B.Br.65-66), Weinstein's adjustment was properly supported by evidence and reasoned expert opinion. *See Finjan*, 626 F.3d at 1210-11 (one-third/two-third profit split not arbitrary based on evidence and reasoned expert opinion). During cross-examination, Weinstein explained that he considered other splits, but concluded 45/55 was appropriate based on the facts in this case. A1708:5-1709:4.

Apple's remaining arguments about calculating the incremental value due to the invention are, at heart, "disagreements [] with [Weinstein's] conclusions, not his methodology." *See i4i*, 598 F.3d at 854 ("*Daubert* and Rule 702 are safeguards against unreliable or irrelevant opinions, not guarantees of correctness."). Similarly, Apple's arguments concerning facts Weinstein used "go to the weight, not admissibility, of his opinion." *Id.* Nonetheless, substantial evidence supports associating the incremental value of adding the front-facing camera to FaceTime, and thus the patented technology; it was added specifically for FaceTime, is essential to FaceTime, was "tuned for FaceTime," and was marketed as a "FaceTime camera." *See, e.g.*, A1719:18-1720:9; A20007; A20013-14; A20727-28. And although 5-10% of FaceTime calls were made via noninfringing relays, all devices forming the basis of the award infringe, and there is no evidence that

5-10% of the devices always made calls through relays. Therefore, the court did not abuse its discretion admitting this theory.

5. Alternative Per-Unit-Royalty Calculation Incorporating Entire Market Value Rule for FaceTime Was Properly Admitted

Finally, Apple argues that Weinstein's final-damages theory—applying the entire market value rule to the portion of iPod Touch sales made because of FaceTime to calculate a per-unit-royalty—was improper because Weinstein did not show VirnetX's patented technology drove demand for Apple's products. B.Br.67. This is incorrect; Apple confuses the issue. *See, e.g.*, B.Br.56-59. VirnetX never claimed its technology drove demand for *all* Apple's products, but a percentage of Apple's sales occurred because of FaceTime. *See, e.g.*, A1640:16-1641:15.

Apple's other criticisms stem from its arguments regarding the NBS split and the misconception that reasonable royalties must be calculated using a royalty rate. B.Br.67-68. That is not the law. *TWM Mfg.*, 789 F.2d at 899-900 (affirming reasonable royalty determined using "analytical approach"); *see also Finjan*, 626 F.3d at 1209-12 (affirming reasonably royalty rate calculated by splitting defendant's associated profits).

Weinstein's theory was reasonable, not speculative, and provides substantial evidence supporting the jury's award. As Weinstein explained, he considered several Apple consumer surveys, and chose the iPod Touch survey to calculate a

per-unit-royalty based on the least-expensive product. A1639:10-1641:5; A1642:12-1643:5. Apple wrongly states that Weinstein (1) claimed this specific survey showed the percentage of *all* iOS devices sold because of FaceTime; and (2) concluded "18% of Apple's mobile device revenue" was attributed to FaceTime. B.Br.19. As explained below, Weinstein did neither and instead used 18% of *iPod Touch* sales revenue in his calculation of a per-unit-royalty.[5] And, this survey did not merely state that FaceTime contributed to sales or was an important feature. Rather, FaceTime was identified as the most desired [redacted] for 18% of individuals [redacted]. A20132.

Using FaceTime surveys is appropriate because substantial evidence shows VirnetX's patents enable FaceTime and there are no commercially viable alternatives—issues Apple does not contest on appeal. *See, e.g.*, A1446:25-1450:8; A1707:18-1708:4; A1789:10-1795:10; A1844:8-1847:20; A2302:18-2303:3. Although other surveys had lower numbers, Weinstein explained this was the most conservative approach due to the iPod Touch's price ($220 versus $649+ for iPhone 4S) and the fact that other products had higher profit margins. *See* A1642:12-1643:5. After determining a reasonable estimate of iPod Touches

[5] Likewise, Weinstein did not "attempt to draw a temporal connection" between Apple's infringing use and increased sales. A1713:22-1714:13; B.Br.58.

sold due to FaceTime, Weinstein calculated the associated profits, accounting for Apple's costs and profit margin derived from Apple's own documents. A1641:16-1642:5; *see also* A1637:3-14. He then applied the NBS split to those incremental profits and divided it by the total number of iPod Touches sold, resulting in an estimated per-unit-royalty. A1642:6-11. Thus, Weinstein's final-damages theory reflects a reasonable per-unit-royalty based on an apportionment of the royalty base given the value of the patented technology.

6. Three Theories Independently Support the Jury's Award

Multiple, legally correct bases fully support the $368M award. *See i4i*, 598 F.3d at 849 ("[W]e will not set aside a general verdict 'simply because the jury *might* have decided on a ground that was supported by insufficient evidence.'" (quoting *Walther v. Lone Star Gas Co.*, 952 F.2d 119, 126 (5th Cir. 1992))). Even if the main theory were unsupported, affirmance is appropriate because (1) VirnetX's alternative FaceTime theories provide damages amounts that independently support the jury's award (A1628:11-1643:23); and (2) Apple's *own* damages theory supports any VPN On Demand portion of the award (*e.g.*, A2288:10-2291:25). Moreover, even if this Court were to affirm the infringement verdict for FaceTime and not VPN On Demand (or vice-versa), substantial evidence still supports the damages award. A1625:5-17; A1628:11-1643:23; A1644:13-22; *see also Energy Transp. Grp., Inc. v. William Demant Holding A/S*,

697 F.3d 1342, 1356-58 (Fed. Cir. 2012)(affirming single award for two patents despite grant of JMOL that one of them was not infringed). Finally, *Uniloc* is inapposite because none of VirnetX's damages theories would skew the damages horizon since none is significantly out of line with the others. *See supra* 29-32.

If Weinstein's testimony is excluded, a new trial is, at a minimum, the appropriate remedy. *See, e.g.*, *Versata*, 717 F.3d at 1267-68 (affirming reasonable-royalty award where plaintiff's damages expert's reasonable-royalty testimony was excluded prior to trial); *Uniloc*, 632 F.3d at 1321 (affirming conditional grant of new trial). Apple cites *Weisgram v. Marley Co.*, but it concerned whether the remaining evidence showed *liability*, not the amount of damages. 528 U.S. 440, 445, 457 (2000). Further, here, VirnetX presented other substantial evidence supporting the award, as discussed above, in addition to Apple's expert's testimony.

VII. CONCLUSION

For the reasons stated above, VirnetX respectfully asks that the Court affirm the entire judgment.

December 2, 2013

Respectfully submitted,

/s/ J. Michael Jakes

J. Michael Jakes
Kara F. Stoll
Srikala P. Atluri
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
901 New York Avenue, NW
Washington, DC 20001-4413
(202) 408-4000

Benjamin R. Schlesinger
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
3500 SunTrust Plaza
303 Peachtree Street, NE
Atlanta, GA 30308-3263
(404) 653-6400

Bradley W. Caldwell
Jason D. Cassady
John Austin Curry
CALDWELL, CASSADY & CURRY
1717 McKinney Avenue
Suite 700
Dallas, TX 75202
(214) 810-4705

Attorneys for VirnetX Inc.

Donald Urrabazo
Arturo Padilla
Ronald Wielkopolski
URRABAZO LAW, P.C.
2029 Century Park East
Suite 1400
Los Angeles, CA 90067
(310) 363-9088

Andy Tindel
MANN, TINDEL & THOMPSON
112 E Line Street, Suite 304
Tyler, TX 75702
(903) 596-0900

Attorneys for Leidos, Inc., formerly Science Applications International Corporation

CERTIFICATE OF SERVICE

I hereby certify that on December 9, 2013, the foregoing **CORRECTED BRIEF FOR PLAINTIFFS-APPELLEES VIRNETX INC. AND SCIENCE APPLICATIONS INTERNATIONAL CORPORATION** was filed via the Court's CM/ECF system. All parties or their counsel who are registered users of the CM/ECF system will receive a notice of this filing from the system. Parties may access this filing through the Court's system. A copy was also served by electronic mail upon counsel for Apple Inc., listed below:

William F. Lee
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
William.Lee@wilmerhale.com

/s/ Kay Wylie, case manager

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing **BRIEF FOR PLAINTIFFS-APPELLEES VIRNETX INC. AND SCIENCE APPLICATIONS INTERNATIONAL INCORPORATED** contains 13,995 words as measured by the word processing software used to prepare this brief.

December 2, 2013

Respectfully submitted,

/s/ J. Michael Jakes

J. Michael Jakes
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, LLP
901 New York Avenue, NW
Washington, DC 20001-4413
(202) 408-4000